ON WILD RAMIFICATION IN REDUCTIONS OF TWO DIMENSIONAL CRYSTALLINE GALOIS

Mavrides, Lambros

Awarding institution:
King's College London

ON WILD RAMIFICATION IN REDUCTIONS OF TWO DIMENSIONAL CRYSTALLINE GALOIS REPRESENTATIONS

By
Lambros Mavrides

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
AT
KING'S COLLEGE LONDON
LONDON, UNITED KINGDOM
JUNE 2016

KING'S COLLEGE LONDON
DEPARTMENT OF MATHEMATICS

The undersigned hereby certify that they have read and recommend to the Faculty of Graduate Studies for acceptance a thesis entitled "**On wild ramification in reductions of two dimensional crystalline Galois representations**" by **Lambros Mavrides** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy**.

Dated: June 2016

Research Supervisor: ______________________
Fred Diamond

Examing Committee: ______________________
Victor Abrashkin

____
Laurent Berger

KING'S COLLEGE LONDON

Date: **June 2016**

Author:	**Lambros Mavrides**
Title:	**On wild ramification in reductions of two dimensional crystalline Galois representations**
Department:	**Department of Mathematics**

Degree: **Ph.D.** Convocation: Year: **2016**

Signature of Author

To Marica, my Pole star

Table of Contents

Table of Contents **v**

Abstract **vii**

Acknowledgements **viii**

1 Introduction & Preliminaries **1**
1.1 Structure of local Galois groups and ramification 4
1.2 Local class field theory 8
1.3 Explicit local class field theory 10
1.4 The Artin-Hasse exponential 18
1.5 Newton polygon 20
1.6 p-adic and mod p Galois representations 22
1.7 The p-adic Hodge theoretic approach to p-adic Galois representations 27
1.8 The theory of field of norms 35
1.9 (ϕ, Γ)-modules in characteristic p 39

2 The Dembélé-Diamond-Roberts conjecture **42**
2.1 The weight part of Buzzard-Diamond-Jarvis in the reducible case . . 43
2.2 Statement of the conjecture in the strongly generic case 46

3 Proof of the Dembélé-Diamond-Roberts conjecture in the strongly generic case **60**
3.1 Computing the representation from the (ϕ, Γ)-module 63
3.2 Distinguished subspaces of $\mathrm{H}^1(G_{X_L}, \overline{\mathbb{F}}_p(\psi))$ 68
3.3 The tamely and wildly ramified splitting fields 75
3.4 The wildly ramified splitting field as a composite of Artin-Schreier extensions 81
3.5 Proof of duality in the equicharacteristic case 85

3.6 Proof of duality in the mixed characteristic case 90

Bibliography **98**

Abstract

Buzzard, Diamond and Jarvis have formulated a generalization of Serre's conjecture regarding mod p representations of the absolute Galois group of a totally real field. Moreover, in the case where the prime p is unramified in the totally real field they conjectured a weight recipe, now a theorem under technical hypotheses (see [15]), regarding the modularity of such representations. This recipe is given in terms of the restriction of the representation to decomposition groups at primes $\mathfrak{p}$ over p. A conjecture of Dembélé, Diamond and Roberts in [8] makes the weight recipe more explicit in the case where p is unramified and the representation restricted to a decomposition group is reducible. In particular they give a description using local class field theory and the Artin-Hasse exponential. In this thesis we look at this conjecture under strong genericity hypotheses of the representation and we give a proof using the work of Chang and Diamond in [7]. In this paper the authors give a description in terms of (ϕ, Γ)-modules. Given that the representation restricted to the decomposition group at $\mathfrak{p}$ acts on the 1 dimensional subspace as χ_1 and on the 1 dimensional quotient as χ_2, we use the equivalence of (ϕ, Γ)-modules with Galois representations to write down explicit cocycles of $\mathrm{H}^1(D_{\mathfrak{p}}, \overline{\mathbb{F}}_p(\chi_1\chi_2^{-1}))$ restricted to the Galois group of the splitting field L of $\chi_1\chi_2^{-1}$. The field of norms gives us an isomorphism between the absolute Galois group of L_∞ and the absolute Galois group of its field of norms X_L, which is an equicharacteristic field. This allows us to do explicit local class field theory using the equicharacteristic splitting field of a cocycle and then transfer this back to the mixed characteristic splitting field and prove the conjecture in the strongly generic case.

Acknowledgements

Firstly I would like to thank my supervisor Professor Fred Diamond for his support throughout this thesis. Without his guidance this thesis wouldn't exist. This thesis is based on his work and his quest for generalizations of Serre's conjecture. It is also based on the work of the French school of algebraic number theorists, which has been a great inspiration to me.

I would like to thank the KCL Graduate School and the Maths Department, for the funding and the support they provided throughout the years. I am also grateful to the A.G. Leventis Foundation for their educational grant which also supported these studies. Many thanks go to my fellow PhD students, especially Sam Derbyshire and Tristan Kalloniatis for many helpful discussions. Thanks also goes to the London Number Theory group, that provides an amazing community for number theorists.

I wish to thank my friends Stelios, Giorgos, Stephanos, Martha, Christos and Irini, for their heartly support. My deepest gratitude goes to my family, Phedias, Chryso, Ioanna and Demos for their unconditional love and for always being there for me. I would also like to thank my wife's family, Stevan, Ljiljana and Marko, for being my second family and my grandparents Takis and Giannoula for being like parents to me. Last but not least, my heartfelt gratitude goes to my new family Marica, for being the most wonderful partner in life I could ever ask for.

Chapter 1

Introduction & Preliminaries

In [26] Serre has formulated a conjecture regarding the modularity of a mod p representation of the absolute Galois group of the rationals. This was proved by Khare and Wintenberger in [18] and [19]. More recently, Buzzard, Diamond and Jarvis have formulated a similar conjecture in [6], regarding the modularity of a mod p representation of the absolute Galois group of a totally real field. More precisely, if F is a totally real number field and

$$\rho : G_F \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

is a continuous, irreducible, totally odd representation, then their conjecture asserts that ρ comes from a Hilbert cuspidal eigenform. If p is unramified in F then a recipe of the possible weights that the cusp form can have is given in their paper, by considering the restriction of ρ to decomposition groups $D_{\mathfrak{p}}$, for primes $\mathfrak{p}|p$. In the case where $\rho|_{D_{\mathfrak{p}}}$ is irreducible, then the recipe is completely explicit. In the case where

$$\rho|_{D_{\mathfrak{p}}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

is reducible, then the recipe is somewhat more indirect and depends on whether the extension class lies in a certain distinguished subspace of $\mathrm{H}^1(D_{\mathfrak{p}}, \overline{\mathbb{F}}_p(\chi_1\chi_2^{-1}))$. The description of these distinguished subspaces is in terms of Hodge-Tate weights of crystalline lifts of $\rho|_{D_\mathfrak{p}}$. However, in [8] the authors make the recipe for the set of weights more explicit. They formulate a conjecture in explicit p-adic Hodge theory about wild ramification in reductions of crystalline Galois representations.

In particular, suppose that ρ is a continuous, irreducible, totally odd representation and $\rho|_{D_\mathfrak{p}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$. Writing S for the set of $\mathbb{F}_p$-linear embeddings $\{k \hookrightarrow \overline{\mathbb{F}}_p\}$ (where k is the residue field of $K := F_\mathfrak{p}$) and fixing $J \subset S$ for which we can write $\chi_1 \mid_{I_K} = \prod_{i=0}^{f-1} \omega_{\tau_i,f}^{a_i} \prod_{j\in J} \omega_{\tau_j,f}^{b_j}$ and $\chi_2 \mid_{I_K} = \prod_{i=0}^{f-1} \omega_{\tau_i,f}^{a_i} \prod_{j\notin J} \omega_{\tau_j,f}^{b_j}$ (see section 1.6 for the definition of $\omega_{\tau_i,f}$). Let $h_i := b_i$, if $i \in J$ and $h_i := -b_i$, if $i \notin J$ and write $\vec{a} = (a_0, ..., a_{f-1})$, $\vec{b} = (b_0, ..., b_{f-1})$, $\vec{d} = (h_0, ..., h_{f-1})$. The weight part of Buzzard-Diamond-Jarvis [6] in the reducible case states that a Serre weight $V_{\vec{a},\vec{b}}$ (see theorem 2.1.1 for the definition of Serre weight) is a weight for the Hilbert modular form for which the representation ρ is modular, precisely when $\rho|_{D_\mathfrak{p}}$ has a crystalline lift with labeled Hodge-Tate weights $\vec{d}$ (see section 1.7 for the definition of crystalline lift with labeled Hodge-Tate weights). The Dembélé-Diamond-Roberts conjecture of [8] reformulates the weight part of Buzzard-Diamond-Jarvis [6] in the reducible case in the following way: given $\vec{d}$ they write down an explicit basis of a quotient of a unit group of the tamely ramified extension. Then they assert that $V_{\vec{a},\vec{b}}$ is a weight for the Hilbert modular form for which the representation is modular precisely when the wildly ramified cocycle of $\mathrm{H}^1(D_\mathfrak{p}, \overline{\mathbb{F}}_p(\chi_1\chi_2^{-1}))$ satisfies a duality property with the explicit basis under local class field theory. This gives the weight part of Buzzard-Diamond-Jarvis in the reducible case a more explicit description.

In this thesis we give a proof of the conjecture of [8] under certain strong genericity assumptions. This involves certain restrictions on $\chi_1\chi_2^{-1}$ including that the character is totally ramified. The proof uses the work of Chang and Diamond [7]. In their paper they write explicit rank two (ϕ, Γ)-modules that correspond under Fontaine's functor to reducible mod p representations that have the property that they have a crystalline lift. Moreover these (ϕ, Γ)-modules are parameterized by $\vec{d}$ of $\chi_1\chi_2^{-1}$ and their crystalline lifts have labeled Hodge-Tate weights equal to $\vec{d}$. Having fixed $J \subset S$ and under certain genericity hypothesis, there exists unique $\vec{a}$, $\vec{b}$ corresponding to $\vec{d}$. Thus representations corresponding to these (ϕ, Γ)-modules have a Serre weight $V_{\vec{a},\vec{b}}$ that corresponds to $\vec{d}$ by the weight part of Buzzard-Diamond-Jarvis. From these (ϕ, Γ)-modules we write down explicit cocycles of $\mathrm{H}^1(D_{\mathfrak{p}}, \overline{\mathbb{F}}_p(\chi_1\chi_2^{-1}))$ parametrized by $\vec{d}$. We then do explicit class field theory on the field of norms of the splitting field of $\chi_1\chi_2^{-1}$ and using the field of norms functor we check that indeed these cocycles satisfy the duality property with respect to the basis elements of the conjecture.

This thesis starts with a preliminaries section, in which we describe the tools we will be using later. Chapter 2 contains a description of the weight part of Buzzard-Diamond-Jarvis [6] in the reducible case. It also contains a description of the Dembélé-Diamond-Roberts conjecture [8] in the strongly generic case. Chapter 3 contains the proof of the Dembélé-Diamond-Roberts conjecture in the strongly generic case. In particular in section 3.1 we compute using Fontaine's functor the representation (proposition 3.1.1) corresponding to the (ϕ, Γ)-modules of Chang and Diamond. In section 3.3 we study the tamely and wildly ramified splitting fields involved. We compute a defining polynomial for the field of norms of the wildly ramified splitting field (proposition 3.2.3) and get a description of the associated cocycle for the equicharacteristic field. In section 3.4 we write the equicharacteristic field as a union of Artin-Schreier extensions (theorem 3.4.1). This allows us to do local class field theory in section 3.5, by computing the Artin-Schreier symbol over the equicharacteristic field (theorem 3.5.5). In particular we write a set of elements of the equicharacteristic field and prove a duality property over the equicharacteristic field (theorem 3.5). We then show in section 3.6 using the theory of field of norms that the duality property over the equicharacteristic field with respect to those elements implies a duality property over the mixed characteristic field with respect to the basis elements of the conjecture (theorem 3.6.12).

1.1 Structure of local Galois groups and ramification

This section gives a brief introduction to the theory of ramification groups. For more details, the reader is referred to Serre's book [24]. For the theory of arithmetically profinite extensions, the reader is referred to Wintenberger's paper [28]. Let L be some finite extension of $\mathbb{Q}_p$. We denote with $\mathcal{O}_L$ its ring of integers, π_L a uniformizer, v_L the unique valuation extending the normalized p-adic valuation, m_L its maximal ideal and k_L its residue field. In the general case where L'/L is not necessarily a finite extension, then we call the extension ***Galois*** if it is a union of finite Galois extensions of L contained in L'. Its Galois group is as usual defined as the automorphism group of L' fixing L. Then one can easily see that $\mathrm{Gal}(L'/L) \cong \varprojlim \mathrm{Gal}(L''/L)$. The inverse limit is taken over the directed set consisting of all finite Galois extensions of L contained in L' ordered by inclusion, and the inverse system sends L'' to $\mathrm{Gal}(L''/L)$ and the inclusion morphisms $M \subset N$ to projections $\mathrm{Gal}(N/L) \longrightarrow \mathrm{Gal}(N/L)/\mathrm{Gal}(N/M) = \mathrm{Gal}(M/L)$. Thus we give the group $\mathrm{Gal}(L'/L)$ the profinite topology, which makes it a Hausdorff, compact, and totally disconnected topological group. The fundamental theorem of Galois theory for finite extensions carries over in this situation as follows. The (contravariant) functors $M \mapsto \mathrm{Gal}(L'/M)$ and $H \mapsto L'^H$ give an equivalence between the category of intermediate fields $L \subset M \subset L'$ with morphisms given by inclusions and the category of closed subgroups $H \subset \mathrm{Gal}(L'/L)$ with morphisms given by inclusions. Moreover the full subcategory of finite (finite and Galois) subextensions of L'/L is equivalent to the full subcategory of open (open and normal) subgroups of $\mathrm{Gal}(L'/L)$. We will be abbreviating with G_L the Galois group of a fixed algebraic closure of the field L and I_L its inertia subgroup.

We now introduce the upper and lower numbering of the ramification groups of a Galois group which will enable us to give it an important filtration. Let us first suppose that $G := \mathrm{Gal}(L'/L)$ is finite. The lower numbering is more straightforward to define;

Definition 1.1.1. Let $i \geq -1$ be an integer. Then we define the ***i-th (lower numbering) ramification group*** of G to be the subgroup

$$G_i(L'/L) := \{g \in G : v_{L'}(ga - a) \geq i + 1, \text{ for all } a \in \mathcal{O}_{L'}\}.$$

This gives a decreasing filtration of G by closed, normal subgroups $G_i(L'/L)$, with $G_i(L'/L) = \{1\}$, for i sufficiently large. We also have $G_{-1}(L'/L) = G$, $G_0(L'/L) = I(L'/L)$ the inertia subgroup of G with fixed field the unramified extension $L'^{\,\mathrm{ur}}$ of L and $G_1(L'/L) = P(L'/L)$ the ***wild ramification subgroup*** of G, with fixed field the tamely ramified extension $L'^{\,\mathrm{tame}}$ of L.

However the lower numbering does not respect quotients and the set $\{G_i(L''/L) : L'' \text{ finite extension of } L \text{ contained in } L'\}$ is not closed under quotients. Thus we don't have transition maps for this set and hence it doesn't make sense to pass to the inverse limit. As a result we cannot use the above construction of infinite Galois groups for infinite ramification groups. To fix this we introduce the upper numbering of the ramification groups, which do respect quotients. We still assume that G is finite. Let x denote a generator of $\mathcal{O}_{L'}$ as an $\mathcal{O}_L$-algebra. Define

$$\begin{aligned} i_G : G &\longrightarrow \mathbb{N} \\ g &\longmapsto v_{L'}(gx - x). \end{aligned}$$

Let $u \geq -1$ be a real number. We define $G_u := G_{\lceil u \rceil}$ and observe that $g \in G_u$ if and only if $i_G(g) \geq u + 1$. Define also the function

$$\begin{aligned} \Phi_{L'/L} : \mathbb{R} \cap [-1, \infty) &\longrightarrow \mathbb{R} \\ u &\longmapsto \textstyle\int_0^u [G_0 : G_t]^{-1} dt. \end{aligned}$$

The convention is to put

$$[G_0 : G_t] := \begin{cases} [G_{-1} : G_0]^{-1}, & \text{if } t = -1 \\ 1, & \text{if } -1 < t \leq 0. \end{cases}$$

As a result $\Phi_{L'/L}(u) = u$, for $-1 \leq u \leq 0$. The function $\Phi_{L'/L}$ is in particular a homeomorphism of $\mathbb{R} \cap [-1, \infty)$ to itself and we denote its inverse by $\Psi_{L'/L}$.

Definition 1.1.2. We define the i***-th (upper numbering) ramification group*** of G to be the subgroup

$$G^v(L'/L) := G_{\Psi_{L'/L}(v)}(L'/L).$$

One can check by a change of variable $w = \Phi_{L'/L}(r)$ that the function $\Psi_{L'/L}$ is given explicitly by

$$\Psi_{L'/L}(v) = \int_0^v [G^0 : G^w] dw.$$

The functions Φ and Ψ satisfy the following transitivity formulas:

Proposition 1.1.3. *For a finite extension L''/L' we have*

$$\Phi_{L''/L} = \Phi_{L''/L'} \circ \Phi_{L'/L} \quad \text{and} \quad \Psi_{L''/L} = \Psi_{L''/L'} \circ \Psi_{L'/L}.$$

Proof. This is Proposition 15 in Chapter IV of [24]. □

We then have the following proposition:

Proposition 1.1.4. *The upper numbering of ramification groups respects quotients in the following sense: Consider a finite Galois extension L''/L contained in L'. Then we have that $G^v(L'/L)Gal(L'/L'')/Gal(L'/L'') \cong G^v(L''/L)$.*

Proof. Chapter IV, Proposition 14, [24]. □

So we can now define ramification groups for infinite extensions. Suppose that L'/L is an infinite Galois extension. Then its upper numbering ramification groups are defined as

$$G^v(L'/L) := \varprojlim G^v(L''/L),$$

where the inverse limit is taken over all finite Galois extensions L''/L contained in L'. The upper numbering ramification groups for infinite extensions also have the following properties: We have a decreasing filtration of G by closed, normal subgroups $G^v(L'/L)$, $G^{-1}(L'/L) = G$, $G^v(L'/L) = I_L$ for $-1 < v \leq 0$ and $\bigcup_{v>0} G^v(L'/L) = P(L'/L)$ the wild ramification subgroup of G.

We can also define lower ramification groups for infinite extensions provided we have the following finiteness condition:

Definition 1.1.5. We call an extension L'/L ***arithmetically profinite*** (abbreviated by ***APF***) if for all $u \geq -1$, the group $G_L^u G_{L'}$ is open in G_L.

So the compactness of the group G implies that the extension L'/L is APF if and only if for all $u \geq -1$, $[G : G^u(L'/L)] < \infty$. In the case where the extension is Galois and APF the functions $\Phi_{L'/L}$ and $\Psi_{L'/L}$ still make sense by putting $\Psi_{L'/L}(v) = \int_0^v [G^0 : G^w] dw$ and $\Phi_{L'/L} := \Psi_{L'/L}^{-1}$. As a result we can define lower ramification groups $G_u(L'/L) := G^{\Phi_{L'/L}(u)}(L'/L)$. We conclude this section with the following definition:

Definition 1.1.6. We call an APF extension L'/L ***strictly APF*** if

$$\liminf_{u \longrightarrow \infty} \frac{\Psi_{L'/L}(u)}{[G^0 : G^u]} > 0.$$

1.2 Local class field theory

In this section we present the main statement of local class field theory. For more information, the reader is referred to Serre's book [24] as well as the book of Fesenko-Vostokov [9]. An important subgroup of the Galois group G_L is the Weil group. Let us denote by k_L the residue field $\mathbb{F}_{p^m}$ of L. Recall that $\overline{k}_L = \bigcup_{t, m|t} \mathbb{F}_{p^t}$ and each $\mathrm{Gal}(\mathbb{F}_{p^t}/\mathbb{F}_{p^m})$ has a canonical generator, namely the p^m-power of the arithmetic Frobenius automorphism, that is $\mathrm{Frob}_p^m : a \mapsto a^{p^m}$. We let $\mathrm{Fr}_p := \mathrm{Frob}_p^{-1}$ be the geometric Frobenius. We then have a homomorphism

$$v : G_L \twoheadrightarrow \varprojlim_{t, m|t} \mathrm{Gal}(L(\zeta_{p^t-1})/L) \xrightarrow{\sim} G_{k_L} = \varprojlim_{t, m|t} \mathrm{Gal}(\mathbb{F}_{p^t}/\mathbb{F}_{p^m}) \xrightarrow{\sim} \hat{\mathbb{Z}}$$

$$g \longmapsto \left(g|_{\mathrm{Gal}(L(\zeta_{p^t-1})/L)}\right)_t \longmapsto \left(\mathrm{Fr}_p^{m v_t(g)}\right)_t \longmapsto (v_t(g))_{\frac{t}{m}}.$$

Recall also that we have a diagonal embedding $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$.

Definition 1.2.1. The ***Weil group*** of G_L is defined to be the subgroup

$$W_L := \{g \in G_L | v(g) \in \mathbb{Z}\}.$$

Observe that in particular $I_L \subset W_L$ and if M/L is finite, then $W_M \subset W_L$. Local class field theory then states the following:

Theorem 1.2.2. *There exists a unique homomorphism*

$$Art_L : L^\times \longrightarrow W_L$$

such that

1. $v \circ Art_L = v_L$;

2. *for any finite abelian extension* L'/L, $Nm_{L'/L}(L'^\times) \subset ker\,(res_{L'} \circ Art_L(L))$ *and* Art_L *induces an isomorphism* $Art_{L'/L} : L^\times/Nm_{L'/L}(L'^\times) \xrightarrow{\sim} Gal(L'/L)$.

Moreover $L^\times \cong W_L^{ab}$ *and the following diagram commutes:*

$$\begin{tikzcd}
W_M^{ab} \arrow[r, "Art_M^{-1}", "\sim"'] \arrow[d] & M^\times \arrow[d, "Nm_{M/L}"] \\
W_L^{ab} \arrow[r, "Art_L^{-1}", "\sim"'] & L^\times
\end{tikzcd}$$

Notice that property 1 implies that uniformizers of L correspond to geometric Frobenius elements. Property 2 implies that $\mathrm{Art}_L^{-1}(W_{L'}) \subset \mathrm{Nm}_{L'/L}(L'^\times)$ and that the following diagram commutes:

$$\begin{tikzcd}
L^\times \arrow[r, "\mathrm{Art}_L", "\sim"'] \arrow[d] & W_L^{\mathrm{ab}} \arrow[d, "\mathrm{Res}_{L'}"] \\
L^\times/\mathrm{Nm}_{L'/L}(L'^\times) \arrow[r, "\mathrm{Art}_{L'/L}", "\sim"'] & \mathrm{Gal}(L'/L)
\end{tikzcd}$$

Let R be a discrete field. Notice that if ψ is a character of W_L over R, then it factors through the quotient W_L^{ab}. We denote the resulting character of W_L^{ab} by $\tilde{\psi}$. Let $\mathrm{Inf}_{W_L^{\mathrm{ab}}}^{W_L}$

denote the inflation map, by pulling back via the map $W_L \longrightarrow W_L^{\mathrm{ab}}$. Then we get a bijective correspondence

$$\{\text{characters of } L^\times \text{ over } R\} \longleftrightarrow \{\text{characters of } W_L \text{ over } R\}$$

$$\chi \longmapsto \mathrm{Inf}_{W_L^{\mathrm{ab}}}^{W_L}(\chi \circ \mathrm{Art}_L^{-1})$$

$$\tilde{\psi} \circ \mathrm{Art}_L \longleftarrow\!\shortmid\, \psi.$$

In the case when we are given a character $\psi : G_L \longrightarrow R^\times$ we have that it has an open kernel. So it factors through a finite quotient of G_L^{ab} and hence through a finite quotient of W_L^{ab}. Precomposing with Art_L we get a character $L^\times \longrightarrow R^\times$.

1.3 Explicit local class field theory

In this section we introduce Kummer and Artin-Schreier theory as well as the Hilbert and Artin-Schreier symbols. As in section 1.2, the reader is referred to Serre's book [24] as well as the book of Fesenko-Vostokov [9]. A class of abelian local field extensions that is relatively easy to describe its class field theory is the class of Kummer extensions. Let us denote by $\mu_n(L)$ the group of the n-th roots of unity in a field L.

Definition 1.3.1. An abelian Galois extension L'/L is called a ***Kummer extension***, if given that it has exponent n (that is its Galois group is n-torsion), $|\mu_n(L)| = n$.

It is easy to see that any subextension of a Kummer extension of exponent n is a Kummer extension of exponent n and that the composite of two Kummer extensions of exponent n is again a Kummer extension of exponent n. As a result we have a maximal Kummer extension of L of exponent n, that we will denote with $L^{\mathrm{Kum},\, n}$. We will also write $G_L^{\mathrm{Kum},\, n}$ for the Galois group $\mathrm{Gal}(L^{\mathrm{Kum},\, n}/L)$.

So given an integer n coprime to the characteristic of L and writing L^{sep} for the separable closure, we have a short exact sequence

$$1 \longrightarrow \mu_n(L) \longrightarrow (L^{\mathrm{sep}})^\times \xrightarrow{x \mapsto x^n} (L^{\mathrm{sep}})^\times \longrightarrow 1 \, .$$

This in turn gives a long exact sequence in cohomology

$$\begin{tikzcd}
1 \arrow[r] & \mu_n(L) \arrow[r] & L^\times \arrow[r, "x \mapsto x^n"] & L^\times \arrow[dll, rounded corners] \\
& \mathrm{H}^1(G_L, \mu_n(L)) \arrow[r] & \mathrm{H}^1(G_L, (L^{\mathrm{sep}})^\times) \arrow[r] & \dots
\end{tikzcd}$$

However, Hilbert's theorem 90 says that $\mathrm{H}^1(G_L, (L^{\mathrm{sep}})^\times) = 0$. Moreover, $\mu_n(L)$ has a trivial G_L action and every homomorphism $G_L \longrightarrow \mu_n(L)$ factors through $G_L^{\mathrm{Kum},\, n}$. Thus $\mathrm{H}^1(G_L, \mu_n(L)) = \mathrm{Hom}(G_L, \mu_n(L)) = \mathrm{Hom}(G_L^{\mathrm{Kum},\, n}, \mu_n(L))$. In particular we have the following theorem:

Theorem 1.3.2. *Suppose $|\mu_n(L)| = n$.*

1. $$\theta : L^\times/(L^\times)^n \xrightarrow{\sim} Hom(G_L^{Kum,\, n}, \mu_n(L))$$

   $$a \longmapsto (g \mapsto \tfrac{g \cdot \alpha}{\alpha}\ ),$$

   where α satisfies $\alpha^n = a$;

2. *Let Δ be a subgroup of $L^\times$ such that $(L^\times)^n \subset \Delta \subset L^\times$ and put $L' := L(\sqrt[n]{\Delta})$. Then L'/L is a Kummer extension of exponent n, and the above isomorphism restricts to an isomorphism*

   $$\theta : \Delta/(L^\times)^n \xrightarrow{\sim} Hom(\,Gal(L'/L), \mu_n(L))\, .$$

As a result, we have the following corollary:

Corollary 1.3.3. *Suppose* $|\mu_n(L)| = n$. *Then we have an inclusion preserving bijection*

$$\begin{aligned}\{\textit{subgroups of } L^\times/(L^\times)^n\} &\longleftrightarrow \{\textit{Kummer extensions of } L \textit{ of exponent } n\}\\ \Delta &\longmapsto L(\sqrt[n]{\Delta})\\ (L')^n \cap L^\times &\longleftarrow\!\shortmid L'.\end{aligned}$$

Proof. Pontryagin duality gives a bijection

$$\begin{aligned}\{\text{closed subgroups of } G_L^{\text{Kum, } n}\} &\longleftrightarrow \{\text{closed subgroups of } \mathrm{Hom}(G_L^{\text{Kum, } n}, \mu_n(L))\}\ ,\\ A &\longmapsto A^\perp := \{h \in \mathrm{Hom}(G_L^{\text{Kum, } n}, \mu_n(L)) :\ \text{for all } g \in A, h(g) = 1\}\\ H^\perp := \{g \in G_L^{\text{Kum, } n} :\ \text{for all } h \in H, h(g) = 1\} &\longleftarrow\!\shortmid H\ .\end{aligned}$$

On the other hand, we have a bilinear map $\theta : L^\times/(L^\times)^n \times G_L^{\text{Kum, n}} \longrightarrow \mu_n(L)$ which induces an isomorphism $L^\times/(L^\times)^n \cong \mathrm{Hom}(G_L^{\text{Kum, } n}, \mu_n(L))$, by theorem 1.3.2. Hence composing the bijection with θ we get a bijection

$$\{\text{closed subgroups of } G_L^{\text{Kum, } n}\} \longleftrightarrow \{\text{subgroups of } L^\times/(L^\times)^n\}\ .$$

Moreover Galois theory gives us an inclusion preserving bijection

$$\begin{aligned}\{\text{Kummer extensions of } L \text{ of exponent } n\} &\longleftrightarrow \{\text{closed subgroups of } G_L^{\text{Kum, } n}\}\ ,\\ L' &\longmapsto \mathrm{Gal}(L^{\text{Kum, } n}/L')\\ (L^{\text{Kum, } n})^H &\longleftarrow\!\shortmid H\ .\end{aligned}$$

Composing these two bijections we get an inclusion preserving bijection

$$\{\text{subgroups of } L^\times/(L^\times)^n\} \longleftrightarrow \{\text{Kummer extensions of } L \text{ of exponent } n\}\ .$$

We now check that the these two correspondences give the stated bijections. If we start with a subextension L'/L of $L^{\text{Kum, }n}/L$, we get $\mathrm{Gal}(L^{\text{Kum, n}}/L')^\perp = \{a \in L^\times/(L^\times)^n :$ for all $g \in \mathrm{Gal}(L^{\text{Kum, n}}/L'), \theta(a,g) = 1\}$. The condition $\theta(a,g) = 1$ is equivalent to $g(\alpha) = \alpha$ for an α with $\alpha^n = a$. But $g(\alpha) = \alpha$ for all $g \in \mathrm{Gal}(L^{\text{Kum, n}}/L')$ is equivalent to $\alpha \in L'$, that is $a \in (L')^n$. Therefore $\mathrm{Gal}(L^{\text{Kum, n}}/L')^\perp = (L')^n \cap L^\times$.

Conversely, given a subgroup $\Delta/(L^\times)^n$ of $L^\times/(L^\times)^n$, we have that $\Delta/(L^\times)^n \cong \mathrm{Hom}(\mathrm{Gal}(L(\sqrt[n]{\Delta})/L), \mu_n(L))$ under θ, by theorem 1.3.2. By Pontryagin duality we get $\{g \in G_L^{\text{Kum, }n} :$ for all $f \in \mathrm{Hom}(\mathrm{Gal}(L(\sqrt[n]{\Delta})/L), \mu_n(L)), f(g) = 1\} = \mathrm{Gal}(L^{\text{Kum, }n}/L(\sqrt[n]{\Delta}))$ and by Galois theory this corresponds to $L(\sqrt[n]{\Delta})$ which is what we wanted. $\square$

Corollary 1.3.4. $L^{\text{Kum, }n} = L(\sqrt[n]{L^\times})$. *Moreover, a Kummer extension of L of exponent n is of the form $L(\sqrt[n]{\Delta})$, for some subgroup Δ of $L^\times/(L^\times)^n$.*

Notice that an easy application of Herbrand's quotient gives that $|L^\times/(L^\times)^n| = \frac{n|\mu_n(L)|}{|n|_L}$. As a result, we have that $L^{\text{Kum, }n}/L$ is in fact a finite extension.

Recall theorem 1.3.2 gives an isomorphism

$$\theta : L^\times/(L^\times)^n \xrightarrow{\sim} \mathrm{Hom}(G_L^{\text{Kum, }n}, \mu_n(L))\ .$$

Recall also theorem 1.2.2, where we have an isomorphism given by the local Artin map

$$\mathrm{Art}_{L^{\text{Kum, }n}/L} : L^\times/\mathrm{Nm}_{L^{\text{Kum, }n}/L}((L^{\text{Kum, }n})^\times) \xrightarrow{\sim} G_L^{\text{Kum, }n}.$$

Thus since $G_L^{\text{Kum, }n}$ has exponent n, so does $L^\times/\mathrm{Nm}_{L^{\text{Kum, }n}/L}((L^{\text{Kum, }n})^\times)$. As a result we have that $(L^\times)^n \subset \mathrm{Nm}_{L^{\text{Kum, }n}/L}((L^{\text{Kum, }n})^\times) \subset L^\times$. Moreover, the two isomorphisms give $\#L^\times/(L^\times)^n = \#G_L^{\text{Kum, }n}$ and $\#L^\times/\mathrm{Nm}_{L^{\text{Kum, }n}/L}((L^{\text{Kum, }n})^\times) = \#G_L^{\text{Kum, }n}$, which gives us that $(L^\times)^n = \mathrm{Nm}_{L^{\mathrm{Kum},\,n}/L}((L^{\mathrm{Kum},\,n})^\times)$. As a result, $\mathrm{Art}_{L^{\mathrm{Kum},\,n}/L}$ combined with the isomorphism θ give the following pairing:

Definition 1.3.5. A ***Hilbert symbol of degree*** n is the pairing

$$(.,.)_n : L^\times \times L^\times \longrightarrow \mu_n(L)$$

$$(a,b) \longmapsto \theta(b)(\mathrm{Art}_{L^{\mathrm{Kum},\,n}/L}(a)) .$$

Thus, unraveling the definition we observe that for an element $\beta = \sqrt[n]{b} \in (L^{\mathrm{Kum},\,n})^\times$ and $a \in L^\times$ we have that $\mathrm{Art}_{L^{\mathrm{Kum},\,n}/L}(a)(\beta) = (a,b)_n\beta$. So computing the Hilbert symbol allows us to explicitly write the local Artin map of a Kummer extension.

Proposition 1.3.6. *The Hilbert symbol satisfies the following properties:*

1. *The Hilbert symbol is multiplicatively bilinear and non-degenerate;*

2. $(a,b) = 1$ *if and only if* a *is a norm from* $L(\sqrt[n]{b})$*;*

3. *The Hilbert symbol is a Steinberg symbol. That is, it also satisfies* $(1-a,a) = (b,1-b) = 1$*, for all* $a,b \in L^\times$*;*

4. *The Hilbert symbol is skew symmetric. That is, it satisfies* $(a,b) = (b,a)^{-1}$*.*

Proof. Parts 1 and 2 follow from the definition of the Hilbert symbol. For 3, notice that $1-a = \prod_{i=1}^n (1-\zeta_n^i \sqrt[n]{a})$ and $1-a$ is a norm from $L(\sqrt[n]{a})$. Hence from 2, we have that $(1-a,a) = 1 = (a,1-a)$. To prove 4, we first claim that $(a,-a) = 1$. First notice that $-a = \frac{1-a}{1-a^{-1}}$. Hence the bilinearity of the symbol implies that $(a,-a) = (a,1-a)(a,(1-a^{-1}))^{-1} = (a,(1-a^{-1}))^{-1}$. But then notice that for any $a,b \in L^\times$, $1 = (aa^{-1},b) = (a,b)(a^{-1},b)$ and so $(a^{-1},b) = (a,b)^{-1}$. Thus $(a,(1-a^{-1}))^{-1} = (a^{-1},(1-a^{-1})) = 1$, which proves the claim. To conclude, we notice that $1 = (ab,-ab) = (a,-a)(a,b)(b,a)(b,-b) = (a,b)(b,a)$. $\square$

This theory can also be extended to equicharacteristic local fields. In particular, since p-th roots of unity are not contained in an equicharacteristic p field, we make the following definition:

Definition 1.3.7. A Galois extension of an equicharacteristic p field that has exponent p, is called an ***Artin-Schreier extension***.

In particular, any subextension of an Artin-Schreier extension is Artin-Schreier, as so is any composite of such extensions. As a result we have a maximal Artin-Schreier extension of an equicharacteristic p field L, that we will denote with L^{AS}. We will also write G_L^{AS} for the Galois group $\mathrm{Gal}(L^{\mathrm{AS}}/L)$. We have a short exact sequence

$$0 \longrightarrow \mathbb{F}_p \longrightarrow L^{\mathrm{sep}} \xrightarrow{x \mapsto x^p - x} L^{\mathrm{sep}} \longrightarrow 0\ ,$$

which in turn gives a long exact sequence in cohomology

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{F}_p \arrow[r] & L \arrow[r, "x \mapsto x^p - x"] & L \arrow[dll, rounded corners] \\ & \mathrm{H}^1(G_L, \mathbb{F}_p) \arrow[r] & \mathrm{H}^1(G_L, L^{\mathrm{sep}}) \arrow[r] & \dots \end{tikzcd}$$

Lemma 1.3.8. *We have that $H^1(G_L, L^{sep}) = 0$.*

Proof. We have that $\mathrm{H}^1(G_L, L^{\mathrm{sep}}) = \varinjlim_{L \subset L' \subset L^{\mathrm{sep}}} \mathrm{H}^1(\mathrm{Gal}(L'/L), L')$, where the extensions L'/L are finite. Hence it suffices to show the result on the finite level. Notice that the normal basis theorem gives us that $L' = L \bigotimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{Gal}(L'/L)]$. Thus L' is a coinduced $\mathrm{Gal}(L'/L)$ module and by Shapiro's lemma, $\mathrm{H}^1(\mathrm{Gal}(L'/L), L') = 0$. $\square$

Since $\mathbb{F}_p$ has a trivial G_L action and every homomorphism $G_L \longrightarrow \mathbb{F}_p$ factors through G_L^{AS}, we have that $\mathrm{H}^1(G_L, \mathbb{F}_p) = \mathrm{Hom}(G_L, \mathbb{F}_p) = \mathrm{Hom}(G_L^{\mathrm{AS}}, \mathbb{F}_p)$. As a result, we have the following theorem:

Theorem 1.3.9. *Suppose L is an equicharacteristic p field.*

1.
$$\iota : L/(Frob_p - 1)L \xrightarrow{\sim} Hom(G_L^{AS}, \mathbb{F}_p)$$
$$a \longmapsto (g \mapsto g \cdot \alpha - \alpha\ ),$$
where α satisfies $\alpha^p - \alpha = a$;

2. *Let Δ be a subgroup of L that contains $(Frob_p - 1)L$ and put $L' := L(\Delta')$, where Δ' is the set of roots of the polynomials $X^p - X - a$, for $a \in \Delta$. Then L'/L is an Artin-Schreier extension and the above isomorphism restricts to an isomorphism*
$$\iota : \Delta/(Frob_p - 1)L \xrightarrow{\sim} Hom(Gal(L'/L), \mathbb{F}_p)\ .$$

Moreover, as in the Kummer theory case, the following holds:

Corollary 1.3.10. 1. *We have an inclusion preserving bijection*
$$\{subgroups\ of\ L/(Frob_p - 1)L\} \longleftrightarrow \{Artin\text{-}Schreier\ extensions\ of\ L\}$$
$$\Delta \longmapsto L(\Delta')$$
$$(Frob_p - 1)L' \cap L \longleftarrow\!\!\dashv L'.$$

2. *Let $\tilde{\Delta}$ be the set of roots of the polynomials $X^p - X - a$, for $a \in L$. Then we have that $L^{AS} = L(\tilde{\Delta})$. Moreover, an Artin-Schreier extension of L is of the form $L(\Delta')$, for some subgroup Δ' of $L/(Frob_p - 1)L$.*

So from theorem 1.3.9 we have an isomorphism
$$\iota : L/(\mathrm{Frob}_p - 1)L \xrightarrow{\sim} \mathrm{Hom}(G_L^{\mathrm{AS}}, \mathbb{F}_p)$$

and we also have the local Artin map

$$\mathrm{Art}_L : L^\times \longrightarrow W_L \; .$$

Combining the two we get:

Definition 1.3.11. The ***Artin-Schreier symbol*** is the pairing

$$(.,.] : L^\times \times L/(\mathrm{Frob}_p - 1)L \longrightarrow \mathbb{F}_p$$

$$(a, b) \longmapsto \mathrm{Art}_{L^{\mathrm{AS}}/L}(a)\, \beta - \beta,$$

where $(\mathrm{Frob}_p - 1)\beta = b$.

As in the case of the Hilbert symbol, the Artin-Schreier symbol also satisfies the following properties:

Proposition 1.3.12. *The Artin-Schreier symbol satisfies the following properties:*

1. $(a_1a_2, b] = (a_1, b] + (a_2, b]$, $(a, b_1 + b_2] = (a, b_1] + (a, b_2]$;
2. $(a, b] = 0$ *if and only if* a *is a norm from* $L(\beta)$*, where* $(Frob_p - 1)\beta = b$*;*
3. $(-a, a] = 0$*, for all* $a \in L^\times$*;*

Proof. Suppose β is a root of $X^p - X - b$.

$$\begin{aligned}
(a_1a_2, b] &= \mathrm{Art}_{L^{\mathrm{AS}}/L}(a_1a_2)\beta - \beta \\
&= \mathrm{Art}_{L^{\mathrm{AS}}/L}(a_1)(\mathrm{Art}_{L^{\mathrm{AS}}/L}(a_2)\beta - \beta) + \mathrm{Art}_{L^{\mathrm{AS}}/L}(a_1)\beta - \beta \\
&= \mathrm{Art}_{L^{\mathrm{AS}}/L}(a_2)\beta - \beta + \mathrm{Art}_{L^{\mathrm{AS}}/L}(a_1)\beta - \beta \\
&= (a_1, b] + (a_2, b],
\end{aligned}$$

since $\mathrm{Art}_{L^{\mathrm{AS}}/L}(a_2)\beta - \beta \in \mathbb{F}_p \subset L$. The second property of (1) follows trivially. Also (2) is a result of kernel of $\mathrm{Art}_{L(\beta)/L}$ being $\mathrm{Nm}_{L(\beta)/L}((L(\beta))^\times)$. For (3) notice that if $a \notin (\mathrm{Frob}_p - 1)L$, then the roots of the polynomial $X^p - X - a$ are not in L. If α is such a root, then $\mathrm{Nm}_{L(\alpha)/L}(-\alpha) = -a$. Hence from (2), we deduce that $(-a, a] = 0$. $\square$

Corollary 1.3.13. *The pairing* $(.,.]$ *factors through*

$$L^\times/(L^\times)^p \times L/(\mathit{Frob}_p - 1)L \longrightarrow \mathbb{F}_p$$

For a prime π of L, given an element $x = \sum_{i>-\infty}^{\infty} x_i \pi^i \in L$, the residue of x with respect to π is defined as $\mathrm{res}_\pi(x) := x_{-1}$. Moreover, we define $\frac{dx}{d\pi} := \sum_{i>-\infty}^{\infty} i x_i \pi^{i-1}$. Then we have the following theorem:

Theorem 1.3.14. *Let* π *be a uniformizer of the equicharacteristic* p *field* L*, which has residue field* k_L*. Then*

$$(a, b] = \mathit{Tr}_{k_L/\mathbb{F}_p}\left(\mathit{res}_\pi\left(\frac{b}{a}\frac{da}{d\pi}\right)\right).$$

Proof. This is theorem 5.6 of chapter IV in [9]. $\square$

1.4 The Artin-Hasse exponential

In this section we introduce the Artin-Hasse exponential. For more details on the subject the reader is referred to Kracht's PhD thesis [20]. For the mod p version, the reader is referred to the paper [21]. Let $L/\mathbb{Q}_p$ be a finite extension with ramification index e and uniformizer π_L. We define the unit groups

$$U_L^i := \ker(\mathcal{O}_L^\times \xrightarrow[\mathrm{mod}\ \pi_L^i]{} (\mathcal{O}_L/\pi_L^i\mathcal{O}_L)^\times) \cong 1 + \pi_L^i\mathcal{O}_L\ .$$

The exponential map $\exp : \pi_L^r \mathcal{O}_L \longrightarrow U_L^r$, defined by $\exp(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}$, converges when $r > \frac{e}{p-1}$ and in fact gives an isomorphism. The Artin-Hasse exponential is a generalization of the exponential map, that converges on the whole of $\mathcal{O}_L$. However, the compromise is that this generalization is not a homomorphism on the whole of $\mathcal{O}_L$.

Definition 1.4.1. Given a prime p, the ***Artin-Hasse exponential*** is the exponential series given by

$$E_p(x) = \exp\left(\sum_{n=0}^{\infty} \frac{x^{p^n}}{p^n}\right).$$

This series has the following properties;

Theorem 1.4.2. *1. The coefficients of the Artin-Hasse exponential series are p-integral. In particular,*

$$E_p(x) = 1 + \sum_{n=1}^{\infty} \frac{|\cup Syl_p(S_n)|}{n!} x^n,$$

where $|\cup Syl_p(S_n)|$ is the number of p-elements in the symmetric group on n letters.

2.

$$E_p(x+y) \equiv E_p(x)E_p(y) \ mod \ (x,y)^p,$$

where $(x,y)^p$ denotes a polynomial in x and y of degree greater or equal to p.

Proof. See theorem 2.10 and lemma 2.11 in [20]. □

By the previous theorem we have that $E_p(x) \in \mathbb{Z}_p[[x]]$ which allows us to define a mod p version of the Artin-Hasse exponential:

Definition 1.4.3. We define the ***mod*** p ***Artin-Hasse exponential*** $\overline{E}_p(x)$, to be the image of $E_p(x) \in \mathbb{Z}_p[[x]]$ in $\mathbb{F}_p[[x]]$ under the map $\mathbb{Z}_p[[x]] \longrightarrow \mathbb{F}_p[[x]]$, given by reducing modulo p.

The mod p Artin-Hasse exponential also satisfies the following important property which is a corollary of theorem 1.4.2:

Corollary 1.4.4.

$$\overline{E}_p(x+y) \equiv \overline{E}_p(x)\overline{E}_p(y) \ mod\ (x,y)^p.$$

1.5 Newton polygon

An important tool in p-adic analysis is the Newton polygon. In this section we provide some results regarding the Newton polygon, that we will need later on. The reader is referred to Gouvêa's book [17] for more details. The Newton polygon is attached to a polynomial over a p-adic field and allows us to deduce several properties of the polynomial.

Definition 1.5.1. Let L be a finite, separable extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((T))$, for a formal variable T and let $f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ be a separable polynomial defined over L. Then the ***Newton polygon*** of f is defined to be the lower convex hull of the set of points $\{(i, v_L(a_i)) : 0 \leq i \leq n, a_i \neq 0\}$.

As a result the Newton polygon consists of line segments $\{l_1, ..., l_k\}$ such that l_j connects the points $(i_j, v_L(a_{i_j}))$ with $(i_{j+1}, v_L(a_{i_{j+1}}))$. We then have the following result.

Theorem 1.5.2. *Let m_j be the slope of l_j and let p_j be the length of the projection of l_j to the horizontal axis. Then there are exactly p_j roots of f in $\overline{L}$ with valuation equal to $-m_j$.*

Proof. First we notice that we can assume that $a_0 = 1$. This is because multiplying f with a constant only causes its Newton polygon to translate vertically (hence m_j and p_j are not affected) and the roots stay the same. So we can factor $f(X) = a_nX^n + ... + a_1X + 1 = (1 - \frac{X}{\alpha_1})...(1 - \frac{X}{\alpha_n})$. Let $\lambda_j := v_L(\frac{1}{\alpha_j})$ and order the α_j so that $\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_n$. Suppose that $\lambda_1 = \lambda_2 = ... = \lambda_r < \lambda_{r+1}$. We want to show that l_1 is the line joining $(0, 0)$ and $(r, v_L(a_r))$, which has slope λ_1. Note that a_j is a symmetric polynomial in the $\frac{1}{\alpha_j}$ and for $i < r$, $v_L(a_i) = v_L(\sum \frac{1}{\alpha_{j_1}...\alpha_{j_i}}) \geq v_L(\frac{1}{\alpha_1...\alpha_i}) \geq i\lambda_1$. So the point $(i, v_L(a_i))$ lies above this line. Moreover, $v_L(a_r) = v_L(\frac{1}{\alpha_1...\alpha_r} + \text{other products}) = v_L(\frac{1}{\alpha_1...\alpha_r}) = r\lambda_1$ and $v_L(a_{r+1}) = v_L(\sum \frac{1}{\alpha_{j_1}...\alpha_{j_{r+1}}}) \geq \frac{1}{\alpha_1...\alpha_r\alpha_{r+1}} > \frac{1}{\alpha_1...\alpha_r\alpha_r} = (r + 1)\lambda_1$. As a result we can conclude that there is a corner in the polygon at $(r, v_L(a_r))$ and l_1 joins $(0, 0)$ and $(r, v_L(a_r))$. But l_1 has slope $m_1 = \lambda_1 = -v_L(\alpha_1)$ and $p_1 = r$ is the number of roots of f of valuation $-m_1$.

We next suppose that $\lambda_{r+1} = ... = \lambda_s < \lambda_{s+1}$. The same argument works to show that l_2 is the line joining $(r, v_L(a_r))$ and $(s, v_L(a_s))$. l_2 has slope $m_2 = \lambda_{r+1} = -v_L(\alpha_{r+1})$ and $p_2 = s - r$ is the number of roots of f of valuation $-m_2$. Continuing in this manner, we verify that the Newton polygon of f has the claimed form. □

From this we get the following corollary.

Corollary 1.5.3. *Suppose f is a monic, separable polynomial over L and that its Newton polygon consists of a single line segment of slope $-\frac{a}{n}$ where a is coprime to n. Then f is irreducible over L.*

Proof. From theorem 1.5.2 we have that f has n roots with valuation $\frac{a}{n}$. Let α be one of the roots. Then we have that $[L(\alpha) : L] \leq n$. Let also e denote the ramification index of $L(\alpha)/L$ and π a uniformizer of $L(\alpha)$. Then we have that $\alpha = u\pi^m$, for some integer m and unit u and $v_L(\alpha) = \frac{a}{n} = \frac{m}{e}$. Since a is coprime to n, we have that n must divide e. Hence $[L(\alpha) : L] = n$. $\square$

From this corollary we can deduce Eisenstein's criterion.

Corollary 1.5.4. *Suppose f is a monic, separable polynomial over L, with $v_L(a_i) \geq 1$ for $0 \leq i \leq n-1$ and $v_L(a_0) = 1$. Then f is irreducible.*

Proof. Since f is monic and $v_L(a_i) \geq 1$ for $0 \leq i \leq n-1$, $v_L(a_0) = 1$, we have that the Newton polygon of f is a single line segment of slope $-\frac{1}{n}$. Hence by corollary 1.5.3, we have that f is irreducible. $\square$

1.6 p-adic and mod p Galois representations

In this section we introduce the notion of a p-adic and mod p Galois representation. For more information the reader is referred to the notes of Berger [2] and Breuil [4].

Definition 1.6.1. A ***p-adic representation*** of G_L is a finite dimensional vector space over $\mathbb{Q}_p$ with a continuous action of G_L.

We can also extend scalars of a p-adic representation to some extension F of $\mathbb{Q}_p$. Let us write $\mathrm{Rep}_F G_L$ for the category of finite dimensional continuous representations of G_L over F. Observe that p-adic representations are of different nature than the l-adic representations where we have that the representation is a finite dimensional vector space over $\mathbb{Q}_l$, for a prime $l \neq p$. The latter representations are essentially 'algebraic' in nature whereas the former have more of a p-adic analytic flavor. This is due to the fact that the wild inertia subgroup of G_L (which is a pro-p subgroup) acts trivially on l-adic vector spaces, but non-trivially on p-adic vector spaces (their topologies match).

Definition 1.6.2. A $\mathbb{Z}_p$***-representation*** of G_L is finitely generated $\mathbb{Z}_p$ -module, with a continuous action of G_L.

As before we can extend scalars to $\mathcal{O}_F$ and write $\mathrm{Rep}_{\mathcal{O}_F} G_L$ for the category of finitely generated continuous representations of G_L over $\mathcal{O}_F$. Our basic example of an object of $\mathrm{Rep}_{\mathcal{O}_F} G_L$ is the p-adic cyclotomic character, given as follows. Let ζ_m denote the primitive m-th root of unity in $\overline{L}$. Then the p-adic cyclotomic character $\chi : G_L \longrightarrow \mathbb{Z}_p^\times$ is defined by $g \cdot \zeta_m = \zeta_m^{\chi(g)}$.

We also have a mod p version of Galois representations.

Definition 1.6.3. A ***mod*** p ***Galois representation*** of G_L is a finite dimensional $\mathbb{F}_p$ vector space with a continuous action of G_L.

As always, we can extend scalars of a mod p representation to some extension $\mathbb{F}$ of $\mathbb{F}_p$ and we write $\mathrm{Rep}_{\mathbb{F}} G_L$ for the category of finite dimensional continuous representations of G_L over $\mathbb{F}$. Any mod p Galois representation is given the discrete topology which implies open kernel and hence any mod p Galois representation factors through the Galois group of some finite extension of L. Our basic example of a mod p Galois representation is the mod p cyclotomic character, given by considering the reduction mod p of the p-adic cyclotomic character χ.

There is a classification of mod p Galois characters over $\overline{\mathbb{F}}_p$, that uses the so called fundamental characters introduced by Serre in [25]. They are constructed as follows. Suppose $\mathbb{F}_{p^m} \subset k_L$ and $L = \mathbb{Q}_p(\zeta_{p^m-1}, \alpha)$, where α is a root of an Eisenstein polynomial over $\mathbb{Q}_p$.

$$\begin{array}{c} L = \mathbb{Q}_p(\zeta_{p^m-1}, \alpha) \\ \Big| \text{ totally ramified} \\ \mathbb{Q}_p(\zeta_{p^m-1}) \\ \Big| \text{ unramified} \\ \mathbb{Q}_p \end{array}$$

Fix an embedding $\tau : k_L \hookrightarrow \overline{\mathbb{F}}_p$ and notice that the extension $L(\sqrt[p^m-1]{\pi_L})/L$ is a Kummer extension.

Definition 1.6.4. We define a ***fundamental character*** of G_L of niveau m with respect to the embedding τ and uniformizer π_L of L be the character $\omega_{\tau,m,\pi_L} : G_L \longrightarrow \overline{\mathbb{F}}_p^\times$ given by

$$\omega_{\tau,m,\pi_L}(g) = \tau\left(\frac{g(\sqrt[p^m-1]{\pi_L})}{\sqrt[p^m-1]{\pi_L}} \bmod \sqrt[p^m-1]{\pi_L}\right).$$

Notice that the restriction of ω_{τ,m,π_L} to I_L is independent of the choice of uniformizer π_L, since replacing π_L with $u\pi_L$ for some $u \in \mathcal{O}_L^\times$ changes ω_{τ,m,π_L} by an unramified character. As a result, when we talk about fundamental characters restricted to inertia, we will not be including the uniformizer in the subscript. In the case where L is an unramified extension of $\mathbb{Q}_p$, we take $\pi_L = -p$. If t divides m, then we have that $L' := L(\sqrt[p^t-1]{\pi_L})$ is a Kummer subextension and so $\omega_{\tau,m,\pi_L}^{\frac{p^m-1}{p^t-1}} = \omega_{\tau',t,\pi_{L'}}$, where $\tau' = \tau^{\frac{p^m-1}{p^t-1}} : \mathbb{F}_{p^t} \hookrightarrow \overline{\mathbb{F}}_p$ and $\pi_{L'} = \pi_L^{\frac{p^m-1}{p^t-1}}$. A special case is the niveau 1 fundamental character, in the case where L is an unramified extension of $\mathbb{Q}_p$. Notice that we have that $\omega_{\tau,m,\pi_L}^{\frac{p^m-1}{p-1}} = \omega_{\tau,m,-p}^{\sum_{i=0}^{m-1} p^i} = \overline{\chi}$. That is a fundamental character of niveau 1 of an unramified extension is the mod p cyclotomic character. This follows from the fact that $L(\zeta_p) = L(\sqrt[p-1]{\pi_L})$.

Now let us fix some embedding $\tau_0 : k_L \hookrightarrow \overline{\mathbb{F}}_p$. Then the rest of the embeddings are gotten by composing with the Frobenius automorphism of $k_L = \mathbb{F}_q$, i.e. $\tau_i := \tau_0 \circ \mathrm{Frob}_p^i = \tau_0^{p^i}$, $0 \leq i \leq m-1$. We then have the following lemma:

Lemma 1.6.5. *Let χ be a continuous character of G_L over $\overline{\mathbb{F}}_p$. Then we have that $\chi|_{I_L}$ factors through a finite, abelian, tamely ramified quotient of degree dividing $p^m - 1$. Moreover, one has*

$$\chi|_{I_L} = \omega_{\tau_0,m}^c = \omega_{\tau_0,m}^{\sum_{i=0}^{m-1} c_i p^i} = \prod_{i=0}^{m-1} \omega_{\tau_i,m}^{c_i},$$

for integers $0 \leq c \leq p^m - 1$ and $0 \leq c_i \leq p-1$ for all i.

Proof. $\chi|_{I_L}$ is continuous and so its kernel is an open subgroup of the compact group I_L. Thus $\chi|_{I_L}$ factors through a finite quotient of I_L. Since the wild inertia P_L is a pro-p subgroup and the image of $\chi|_{I_L}$ has size prime to p, we have that $P_L \subset \ker\chi|_{I_L}$. So $\chi|_{I_L}$ factors through a finite, abelian, tamely ramified quotient G of I_L. Let us suppose that the image of $\chi|_{I_L}$ is contained in $\mathbb{F}_{p^n}^\times$, for n as small as possible. We may consider the field $L' := \mathbb{Q}_p(\zeta_{p^n-1}, \alpha)$, which has $I_L = I_{L'}$ and $k_{L'} = \mathbb{F}_{p^n}$. We get by Kummer theory that G is a quotient of $\mathrm{Gal}(L'(\sqrt[p^n-1]{\pi_L})/L') \cong \mathbb{F}_{p^n}^\times$ and $\chi|_{I_L} = \omega_{\tau,n}^r$, for some $0 \leq r \leq p^n - 1$.

We now want to show that n divides m. Notice that we have a surjection $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L(\sqrt[p^n-1]{\pi_L})) \twoheadrightarrow G_{k_L}$, and so we take a lifting $s \in G_L$ of Frob_p^m, fixing $\sqrt[p^n-1]{\pi_L}$. Since $\omega_{\tau,n}$ extends to G_L, we have that $\omega_{\tau,n}(sgs^{-1}) = \omega_{\tau,n}(g)$. Moreover since I_L is normal in G_L, we have that $sgs^{-1} \in I_L$ and so $\omega_{\tau,n}(sgs^{-1}) = \tau\left(\frac{sgs^{-1}(\sqrt[p^n-1]{\pi_L})}{\sqrt[p^n-1]{\pi_L}} \bmod \sqrt[p^n-1]{\pi_L}\right) = \tau\left(\left(\frac{g(\sqrt[p^n-1]{\pi_L})}{\sqrt[p^n-1]{\pi_L}}\right)^{p^m} \bmod \sqrt[p^n-1]{\pi_L}\right) = \omega_{\tau,n}(g)^{p^m}$. Hence $\omega_{\tau,n}(g) = \omega_{\tau,n}(g)^{p^m}$, for any $g \in I_L$. So we have that n divides m. Using $\omega_{\tau,n} = \omega_{\tau_i,m}^{\frac{p^m-1}{p^n-1}}$ for some i and $\tau_i = \tau_0^{p^i}$ we have that $\chi|_{I_L} = \omega_{\tau_0,m}^c$, where $c = rp^i\frac{p^m-1}{p^n-1}$. $\square$

Definition 1.6.6. Let χ be a continuous character of G_L over $\overline{\mathbb{F}}_p$. Then by lemma 1.6.5, one has that $\chi|_{I_L} = \omega^c_{\tau_0,m} = \omega^{\sum_{i=0}^{m-1} c_i p^i}_{\tau_0,m}$, for integers $0 \leq c \leq p^m - 1$ and $0 \leq c_i \leq p-1$ for all i. We define $(c_0, ..., c_{m-1})$ to be the ***tame signature*** of χ. So the tame signature of χ is an element of the set $T := \{1, 2, ..., p-1\}^m$.

Let us define an action of $\mathrm{Gal}(k_L/\mathbb{F}_p)$ on the set T by the formula $\mathrm{Frob}_p \cdot (c_0, c_1, ..., c_{m-1}) = (c_{m-1}, c_{f-1}, ..., c_0)$. Note that if χ has tame signature $\vec{c}$, then $\mathrm{Frob}_p \circ \chi$ has tame signature $\mathrm{Frob}_p(\vec{c})$.

Definition 1.6.7. We define the ***period*** of $\vec{c} \in T$ to be the cardinality of its orbit in $\mathrm{Gal}(k_L/\mathbb{F}_p)$. Moreover, we define the ***absolute niveau*** of χ to be the period of its tame signature. In case that χ has absolute niveau m, then we say χ is ***primitive***.

Notice that the orbit of the tame signature of χ under $\mathrm{Gal}(k_L/\mathbb{F}_p)$ is independent of the choice of the embedding τ_0.

Recall that $G_{k_L} := \mathrm{Gal}(\overline{k_L}/k_L)$ is isomorphic to $\hat{\mathbb{Z}}$ with a generator being the m-th power of the geometric Frobenius automorphism, $\mathrm{Fr}_p^m : \alpha \mapsto \alpha^{-q}$. Hence a character $G_{k_L} \longrightarrow \overline{\mathbb{F}}_p^\times$ is determined by where it sends Fr_p^m to, say to some element $x \in \overline{\mathbb{F}}_p^\times$. We denote the inflation of this character to G_L by unr_x. Since the sequence

$$1 \longrightarrow I_L \longrightarrow G_L \longrightarrow G_{k_L} \longrightarrow 1$$

is exact, we have the following.

Corollary 1.6.8. *Any character $\chi : G_L \longrightarrow \overline{\mathbb{F}}_p^\times$ is in fact equal to $\omega^c_{\tau_0,n,\pi_L} unr_x$, for some uniformizer π_L of L, some integer n dividing m, $0 \leq c \leq p^n - 1$ and $x \in \overline{\mathbb{F}}_p^\times$.*

We can pass from the category $\mathrm{Rep}_F G_L$ to the category $\mathrm{Rep}_{\mathbb{F}} G_L$, using the following lemma:

Lemma 1.6.9. *Let V be an object of $Rep_F G_L$. Then there exists an object T of $Rep_{\mathcal{O}_F} G_L$ which is a lattice of V.*

Proof. Suppose $\dim_F V = n$ and pick a basis $B := \{e_1, .., e_n\}$. Put T_0 for the module spanned by B over $\mathcal{O}_F$. Notice that by continuity $\mathrm{Stab}_{G_L} e_i \subset G_L$ is open for all i. Put $U := \cap_{i=1}^n \mathrm{Stab}_{G_L} e_i$ which is also open in G_L and hence of finite index. Define T_1 to be the $\mathcal{O}_F$ span of the elements $\{ge_i\}_{1 \le i \le n, g \in G/U}$, and this gives us a finitely generated $\mathcal{O}_F[G_L]$-stable lattice of V. □

Hence given an object V of $\mathrm{Rep}_F G_L$ we can find an object T of $\mathrm{Rep}_{\mathcal{O}_F} G_L$ as in the above lemma, reduce modulo the maximal ideal m_F and get an object $\overline{T}$ of $\mathrm{Rep}_{k_F} G_L$.

1.7 The p-adic Hodge theoretic approach to p-adic Galois representations

This section provides an introduction to p-adic Hodge theory. For more information the reader is referred to the original papers of Fontaine [11], [14], [12], as well as the notes of Berger [2] and Brinon-Conrad [5]. We begin by defining some period rings of Fontaine we will need. L will denote some finite extension of $\mathbb{Q}_p$ and $\mathbb{C}_p$ the p-adic completion of $\overline{\mathbb{Q}}_p$. The action of $G_{\mathbb{Q}_p}$ on $\overline{\mathbb{Q}}_p$ extends uniquely and continuously on $\mathbb{C}_p$. Let $\chi : G_{\mathbb{Q}_p} \longrightarrow \overline{\mathbb{Z}}_p^\times$ be the p-adic cyclotomic character and denote its reduction mod p by $\overline{\chi}$. Let H_L denote the kernel of the cyclotomic character restricted at G_L and $\Gamma_L := G_L/H_L$. e will denote the basis element of the 1-dimensional $\mathbb{C}_p$-vector space for which $g \cdot e := \chi(g)e$, where $g \in G_L$. More generally, if $n \in \mathbb{Z}$, then we write $\mathbb{C}_p(n)$ for the 1-dimensional $\mathbb{C}_p$-vector space with basis element e^n. Then it is a theorem of Tate and Sen ([22] and [27]) that $\mathbb{C}_p(n)^{G_L} = 0$, for $n \neq 0$ and $\mathbb{C}_p^{G_L} = L$. The first period ring we define, is the ***Hodge-Tate period ring***. This is a $\mathbb{Z}$-graded ring, defined by $\mathbb{B}_{\mathrm{HT}} := \bigoplus_{n\in\mathbb{Z}} \mathbb{C}_p(n)$, with multiplication given by $\mathbb{C}_p(n) \bigotimes_{\mathbb{C}_p} \mathbb{C}_p(n') \cong \mathbb{C}_p(n+n')$. Let us also write Gr_L for the category of finite dimensional L-vector spaces which have a $\mathbb{Z}$-grading. Given an object of $\mathrm{Rep}_F G_L$, we can consider it as an object of $\mathrm{Rep}_{\mathbb{Q}_p} G_L$, via the functor which forgets the F-action. Then we have a covariant functor

$$\mathbf{D}_{\mathrm{HT}} : \mathrm{Rep}_{\mathbb{Q}_p} G_L \longrightarrow \mathrm{Gr}_L$$

$$V \longmapsto (V \bigotimes_{\mathbb{Q}_p} \mathbb{B}_{\mathrm{HT}})^{G_L}.$$

Let us denote by $V\{n\} = \mathrm{gr}^n(\mathbf{D}_{\mathrm{HT}}(V)) := (V \bigotimes_{\mathbb{Q}_p} \mathbb{C}_p(n))^{G_L}$, the n-th graded piece of $\mathbf{D}_{\mathrm{HT}}(V)$. Then $V\{n\} = L^{\dim V\{n\}}$ with trivial G_L-action can also be viewed as an object of $\mathrm{Rep}_L G_L$. Then we have the following lemma of Serre and Tate:

Lemma 1.7.1. *For V an object of $Rep_{\mathbb{Q}_p} G_L$, we have an injection*

$$\bigoplus_{n\in\mathbb{Z}} \left(\mathbb{C}_p(-n) \bigotimes_L V\{n\} \right) \hookrightarrow V \bigotimes_{\mathbb{Q}_p} \mathbb{C}_p$$

as a morphism in the category $Rep_{\mathbb{C}_p} G_L$.

In particular, this lemma implies that $\dim_L \mathbf{D}_{\mathrm{HT}}(V) \leq \dim_{\mathbb{Q}_p} V$. The above injection is in fact an isomorphism if and only if the previous inequality is in fact an equality. This motivates the following definition:

Definition 1.7.2. Let V be an object of $\mathrm{Rep}_{\mathbb{Q}_p} G_L$. Then we say that V is ***Hodge-Tate*** if $\dim_L \mathbf{D}_{\mathrm{HT}}(V) = \dim_{\mathbb{Q}_p} V$. We write $\mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{HT}} G_L$ for the full subcategory of $\mathrm{Rep}_{\mathbb{Q}_p} G_L$ whose objects are Hodge-Tate.

So let V be an object of $\mathrm{Rep}^{\mathrm{HT}}_{\mathbb{Q}_p} G_L$. Then the above lemma says that

$$V \bigotimes_{\mathbb{Q}_p} \mathbb{C}_p \cong \bigoplus_{n \in \mathbb{Z}} \mathbb{C}_p(n)^{\dim V\{-n\}}$$

with $V\{-n\} = 0$ for all but finitely many integers n. Then we call an integer n a ***Hodge-Tate weight*** of V, if $V\{-n\} \neq 0$. Moreover the multiplicity of this Hodge-Tate weight is given by $\dim V\{-n\}$. The above lemma also implies that $\dim V\{-n\}$ is finite for all integers n. Hence an object V in $\mathrm{Rep}^{\mathrm{HT}}_{\mathbb{Q}_p} G_L$ has finitely many Hodge-Tate weights and each with finite multiplicity. In particular, the number of Hodge-Tate weights of V counted with multiplicity, is equal to the dimension of V. For example, if $V = \chi$ is the p-adic cyclotomic character, then we see that by the theorem of Tate-Sen, χ is Hodge-Tate, with Hodge-Tate weight equal to 1, with multiplicity 1.

As a final remark we note that the above constructions were motivated from geometry. Let X be some smooth proper scheme over L. Then its étale cohomology groups $\mathrm{H}^r_{\acute{e}t}(X_{\overline{L}}, \mathbb{Q}_p)$ are objects of $\mathrm{Rep}_{\mathbb{Q}_p} G_L$, whereas its Hodge cohomology groups $\mathrm{H}^r(X, \Omega^n)$ have the trivial G_L-action. A theorem due to Faltings compares the étale cohomology of X with its Hodge cohomology;

$$\mathrm{H}^r_{\acute{e}t}(X_{\overline{L}}, \mathbb{Q}_p) \bigotimes_{\mathbb{Q}_p} \mathbb{C}_p \xrightarrow{\sim} \bigoplus_{n \in \mathbb{Z}} (\mathbb{C}_p(-n) \bigotimes_L \mathrm{H}^{r-n}(X, \Omega^n)).$$

In particular this implies that

$$\mathrm{H}^r_{\acute{e}t}(X_{\overline{L}}, \mathbb{Q}_p)\{n\} \cong \mathrm{H}^{r-n}(X, \Omega^n)$$

and thus

$$\mathbf{D}_{\mathrm{HT}}(\mathrm{H}^r_{\acute{e}t}(X_{\overline{L}}, \mathbb{Q}_p)) \cong \mathrm{H}^r(X) := \bigoplus_{n \in \mathbb{Z}} \mathrm{H}^{r-n}(X, \Omega^n).$$

In other words $\mathrm{H}^r_{\acute{e}t}(X_{\overline{L}}, \mathbb{Q}_p)$ is Hodge-Tate. A natural question is whether we can do the same for the algebraic de Rham cohomology of X, that is whether we can find some period ring whose associated functor gives

$$\mathbf{D}_{\mathrm{dR}}(\mathrm{H}^r_{\acute{e}t}(X_{\overline{L}}, \mathbb{Q}_p)) \cong \mathrm{H}^r_{\mathrm{dR}}(X).$$

It turns out that such a period ring exists and the next thing we do is to define it. We will also define the crystalline period ring, which provides an analogue of the Néron-Ogg-Shafarevich criterion for the p-adic case. That is given an abelian variety A over L, then the l-adic version of the criterion says that A has good reduction over L if and only if for any $l \neq p$, the inertia subgroup I_L of G_L acts trivially on the dual vector space $\mathrm{H}^1_{\acute{e}t}(A_{\overline{L}}, \mathbb{Q}_l)$. The p-adic version of this turns out to be that A has good reduction over L if and only if the p-adic dual representation of $\mathrm{H}^1_{\acute{e}t}(A_{\overline{L}}, \mathbb{Q}_p)$ is crystalline.

First we need to introduce some intermediate rings that we need in defining the de Rham period ring. So first let

$$\tilde{\mathbb{E}} := \varprojlim_{x \mapsto x^p} \mathbb{C}_p = \{(x^{(0)}, x^{(1)}, ...) \mid (x^{(i+1)})^p = x^{(i)}\}.$$

Let $x = (x^{(i)})$, $y = (y^{(i)})$ be two elements of $\tilde{\mathbb{E}}$. The ring structure on $\tilde{\mathbb{E}}$ is given by setting $(x+y)^{(i)} := \lim_{j \longrightarrow \infty} (x^{(i+j)} + y^{(i+j)})^{p^j}$ and $(xy)^{(i)} := x^{(i)} y^{(i)}$. In particular this makes $\tilde{\mathbb{E}}$ a characteristic p ring, with an action of Frobenius ϕ given by $\phi((x^{(i)})) := ((x^{(i)})^p)$ and an action of $g \in G_{\mathbb{Q}_p}$ given by $g((x^{(i)})) := (g(x^{(i)}))$. We define a valuation on $\tilde{\mathbb{E}}$ by putting $v_E(x) := v_p(x^{(0)})$. Thus we may let $\tilde{\mathbb{E}}^+$ to be the ring of integers of $\tilde{\mathbb{E}}$. $\tilde{\mathbb{E}}$ has a $G_{\mathbb{Q}_p}$ action and we define $\tilde{\mathbb{E}}_L := \tilde{\mathbb{E}}^{H_L}$. There is a choice of a distinguished element of $\tilde{\mathbb{E}}$ namely $\epsilon := (\zeta_{p^i})$ where ζ_{p^i} is a primitive p^i-th root of unity for all $i \geq 1$ and $\zeta_{p^0} = 1$. Then we have that since $v(\zeta_{p^i} - 1) = \frac{1}{(p-1)p^{i-1}}$, $v_E(\epsilon - 1) = v((\epsilon-1)^{(0)}) = v(\lim_{j \longrightarrow \infty} (\zeta_{p^j} - 1)^{p^j}) = \lim_{j \longrightarrow \infty} p^j v(\zeta_{p^j} - 1) = \lim_{j \longrightarrow \infty} p^j \frac{1}{(p-1)p^{j-1}} = \frac{p}{p-1}$. Next we define $\pi := \epsilon - 1$ and we put $\mathbb{E}_{\mathbb{Q}_p} := \mathbb{F}_p((\pi))$, as a subfield of $\tilde{\mathbb{E}}$. Then we define $\mathbb{E}$

to be the separable closure of $\mathbb{E}_{\mathbb{Q}_p}$ in $\tilde{\mathbb{E}}$ and $\mathbb{E}^+$ to be the ring of integers of $\mathbb{E}$. Notice that $\mathbb{E}$ has a $G_{\mathbb{Q}_p}$ action and for $H_L = \mathrm{Gal}(\overline{L}/L_\infty)$, one has that $\mathbb{E}_{\mathbb{Q}_p} = \mathbb{E}^{H_{\mathbb{Q}_p}}$. This allows us to define $\mathbb{E}_L := \mathbb{E}^{H_L}$ and $\mathbb{E}_L^+$ for its ring of integers. In particular, we have that $H_L \cong \mathrm{Gal}(\mathbb{E}/\mathbb{E}_L) = G_{\mathbb{E}_L}$.

We now move on to some period rings of characteristic 0. Let us denote by $\tilde{\mathbb{A}}^+ := W(\tilde{\mathbb{E}}^+)$, the Witt vectors of $\tilde{\mathbb{E}}^+$. Let $[x] \in \tilde{\mathbb{A}}^+$ denote the Teichmüller lift of $x \in \tilde{\mathbb{E}}^+$ and $\pi := [\epsilon] - 1$. Now put $\tilde{\mathbb{A}} := \tilde{\mathbb{A}}^+[\frac{1}{\pi}]$ and $\tilde{\mathbb{B}}^+ := \tilde{\mathbb{A}}^+[\frac{1}{p}] = \{\sum_{k>>-\infty} p^k[x_k] | x_k \in \tilde{\mathbb{E}}^+\}$, $\tilde{\mathbb{B}} := \tilde{\mathbb{A}}[\frac{1}{p}]$. By functoriality properties of these constructions, the rings $\tilde{\mathbb{A}}^+$ and $\tilde{\mathbb{B}}^+$ both inherit an action of $G_{\mathbb{Q}_p}$. Notice that in particular, using the Frobenius morphism of the Witt vectors, one has that these rings have a Frobenius action ϕ as well. Then let $\theta : \tilde{\mathbb{A}}^+ \longrightarrow \mathcal{O}_{\mathbb{C}_p}$ be the homomorphism $\sum_{k\geq 0} p^k[x_k] \mapsto \sum_{k\geq 0} p^k x_k^{(0)}$, induced by the map $\tilde{\mathbb{E}}^+ \longrightarrow \mathcal{O}_{\mathbb{C}_p}/p$, given by $(x^{(i)}) \mapsto x^{(0)}$. We extend this to a surjective homomorphism $\theta : \tilde{\mathbb{B}}^+ \longrightarrow \mathbb{C}_p$, by defining $\sum_{k>>-\infty} p^k[x_k] \mapsto \sum_{k>>-\infty} p^k x_k^{(0)}$. The kernel of this map is the ideal generated by the element $\omega := \frac{\pi}{\phi^{-1}(\pi)} = \frac{[\epsilon]-1}{[\epsilon_1]-1}$, where $\epsilon_1 := (\epsilon^{(1)}, \epsilon^{(2)}, ...)$.

Let us define $\mathbb{B}_{\mathrm{dR}}^+$ to be the ω-adic completion of $\tilde{\mathbb{B}}^+$, i.e. $\mathbb{B}_{\mathrm{dR}}^+ := \varprojlim_n (\tilde{\mathbb{B}}^+/(\omega)^n)$, which is a complete discrete valuation ring with residue field $\mathbb{C}_p$. Then by continuity θ extends to a homomorphism $\theta : \mathbb{B}_{\mathrm{dR}}^+ \longrightarrow \mathbb{C}_p$. There is a distinguished element of this ring, namely $t := \log([\epsilon]) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{\pi^n}{n}$. Observe that indeed this series converges in $\mathbb{B}_{\mathrm{dR}}^+$, since $\theta(\pi) = 0$ and hence π is 'small' in the ω-adic topology of $\mathbb{B}_{\mathrm{dR}}^+$. This element is indeed a uniformizer of $\mathbb{B}_{\mathrm{dR}}^+$ and also has the property that $\sigma \in G_{\mathbb{Q}_p}$ acts on it via the cyclotomic character; $\sigma(t) = \sigma(\log([\epsilon])) = \log(\sigma([\epsilon])) = \log([\epsilon^{\chi(\sigma)}]) = \chi(\sigma)t$. We define the ***de Rham period ring*** to be the field $\mathbb{B}_{\mathrm{dR}} := \mathbb{B}_{\mathrm{dR}}^+[\frac{1}{t}]$. $\mathbb{B}_{\mathrm{dR}}$ also carries a natural decreasing, separated, exhaustive filtration given by $\mathrm{Fil}^i \mathbb{B}_{\mathrm{dR}} = t^i \mathbb{B}_{\mathrm{dR}}^+$, $i \in \mathbb{Z}$, which makes it a filtered field. One can show that $\mathbb{B}_{\mathrm{dR}}^{G_L} = L$. Let us denote by $\mathrm{MF}_{\mathbb{Q}_p}$

the category of finite dimensional vector spaces over $\mathbb{Q}_p$, which have a decreasing, separated and exhaustive filtration. Then there is a functor $\mathrm{gr} : \mathrm{MF}_{\mathbb{Q}_p} \longrightarrow \mathrm{Gr}_{\mathbb{Q}_p}$ defined by $V \mapsto \bigoplus_{i\in\mathbb{Z}} \left(\mathrm{Fil}^i V/\mathrm{Fil}^{i+1} V\right)$. Using this functor along with the properties of t and the homomorphism θ, we get a graded vector space associated to $\mathbb{B}_{\mathrm{dR}}$, which turns out to be isomorphic to $\mathbb{B}_{\mathrm{HT}}$; $\mathrm{gr}(\mathbb{B}_{\mathrm{dR}}) = \bigoplus_{i\in\mathbb{Z}}(t^i\mathbb{B}^+_{\mathrm{dR}}/t^{i+1}\mathbb{B}^+_{\mathrm{dR}}) \cong \mathbb{B}_{\mathrm{HT}}$ and for the i-th graded piece we have $\mathrm{gr}^i(\mathbb{B}_{\mathrm{dR}}) := t^i\mathbb{B}^+_{\mathrm{dR}}/t^{i+1}\mathbb{B}^+_{\mathrm{dR}} \cong \mathbb{C}_p(i)$. A disadvantage of the de Rham period ring is that it does not have a Frobenius action and hence we will isolate a subring which affords such an action.

So let $\mathbb{A}_{\mathrm{cris}} := \{\sum_{n\geq 0} a_n \frac{\omega^n}{n!} \in \mathbb{B}^+_{\mathrm{dR}} \mid a_n \in \tilde{\mathbb{A}}^+, a_n \underset{n\longrightarrow\infty}{\longrightarrow} 0\}$ and $\mathbb{B}^+_{\mathrm{cris}} := \mathbb{A}_{\mathrm{cris}}[\frac{1}{p}]$, which is indeed closed under the action of $G_{\mathbb{Q}_p}$. Notice that $t \in \mathbb{B}^+_{\mathrm{cris}}$ and so we define the ***crystalline period ring*** to be the ring $\mathbb{B}_{\mathrm{cris}} := \mathbb{B}^+_{\mathrm{cris}}[\frac{1}{t}]$, a subring of $\mathbb{B}_{\mathrm{dR}}$ with actions of ϕ and $G_{\mathbb{Q}_p}$ and a filtration inherited from $\mathbb{B}_{\mathrm{dR}}$, i.e. $\mathrm{Fil}^i\mathbb{B}_{\mathrm{cris}} := \mathrm{Fil}^i\mathbb{B}_{\mathrm{dR}} \cap \mathbb{B}_{\mathrm{cris}}$. One can show that $\mathbb{B}^{G_L}_{\mathrm{cris}} = L_0$, where L_0 is the maximal absolutely unramified subfield of L.

Let us now introduce another category. Let us denote by MF_L the category of finite dimensional vector spaces over L, which have a decreasing, separated and exhaustive filtration. Now let $\mathrm{MF}^{\phi}_{L_0}$ be the category whose objects are finite dimensional vector spaces over L_0 which have a semilinear Frobenius action ϕ and such that $V \bigotimes_{L_0} L$ has a decreasing, separated and exhaustive filtration. Let us consider the following covariant functors:

$$\mathbf{D}_{\mathrm{dR}} : \mathrm{Rep}_{\mathbb{Q}_p} G_L \longrightarrow \mathrm{MF}_L$$

$$V \longmapsto (V \bigotimes_{\mathbb{Q}_p} \mathbb{B}_{\mathrm{dR}})^{G_L},$$

$$\mathbf{D}_{\text{cris}} : \text{Rep}_{\mathbb{Q}_p} G_L \longrightarrow \text{MF}^{\phi}_{L_0}$$

$$V \longmapsto (V \bigotimes_{\mathbb{Q}_p} \mathbb{B}_{\text{cris}})^{G_L}.$$

One can easily see that $\dim_L \mathbf{D}_{\text{dR}}(V) \leq \dim_{\mathbb{Q}_p} V$ and $\dim_{L_0} \mathbf{D}_{\text{cris}}(V) \leq \dim_{\mathbb{Q}_p} V$. The filtration on $\mathbf{D}_{\text{dR}}(V)$ and $\mathbf{D}_{\text{cris}}(V) \bigotimes_{L_0} L$ is inherited by the filtration of the rings $\mathbb{B}_{\text{dR}}$ and $\mathbb{B}_{\text{cris}}$. Also the action of Frobenius on $\mathbf{D}_{\text{cris}}(V)$ is inherited from the action of Frobenius on $\mathbb{B}_{\text{cris}}$.

Definition 1.7.3. We say that an object V of $\text{Rep}_{\mathbb{Q}_p} G_L$ is ***de Rham*** (resp. ***crystalline***), if $\dim_L \mathbf{D}_{\text{dR}}(V) = \dim_{\mathbb{Q}_p} V$ (resp. $\dim_{L_0} \mathbf{D}_{\text{cris}}(V) = \dim_{\mathbb{Q}_p} V$). We write $\text{Rep}^{\text{dR}}_{\mathbb{Q}_p} G_L$ and $\text{Rep}^{\text{cris}}_{\mathbb{Q}_p} G_L$ for the corresponding full subcategories of $\text{Rep}_{\mathbb{Q}_p} G_L$.

We remark that these subcategories are in fact stable under sub-quotients, direct sums and tensor products. In general we have that $\mathbf{D}_{\text{cris}}(V) \bigotimes_{L_0} L \hookrightarrow \mathbf{D}_{\text{dR}}(V)$ and thus $\dim_{L_0} \mathbf{D}_{\text{cris}}(V) \leq \dim_L \mathbf{D}_{\text{dR}}(V)$, which implies that a crystalline representation is necessarily de Rham.

Recall that we had that $\text{gr}(\mathbb{B}_{\text{dR}}) \cong \mathbb{B}_{\text{HT}}$ and this implies

$$\left(\text{gr}(\mathbb{B}_{\text{dR}}) \bigotimes_{\mathbb{Q}_p} V \right)^{G_L} \cong \left(\mathbb{B}_{\text{HT}} \bigotimes_{\mathbb{Q}_p} V \right)^{G_L} = \mathbf{D}_{\text{HT}}(V).$$

In general we have that

$$\text{gr}(\mathbf{D}_{\text{dR}}(V)) \subset \mathbf{D}_{\text{HT}}(V).$$

Moreover, $\dim \text{gr}(\mathbf{D}_{\text{dR}}(V)) = \dim \mathbf{D}_{\text{dR}}(V)$, thus $\dim \mathbf{D}_{\text{dR}}(V) \leq \dim \mathbf{D}_{\text{HT}}(V)$. So we get that if V is de Rham, then it is in fact Hodge-Tate. So to summarize we have the following hierarchy of p-adic Galois representations:

$$\text{Rep}^{\text{cris}}_{\mathbb{Q}_p} G_L \quad \subset \quad \text{Rep}^{\text{dR}}_{\mathbb{Q}_p} G_L \quad \subset \quad \text{Rep}^{\text{HT}}_{\mathbb{Q}_p} G_L \quad \subset \quad \text{Rep}_{\mathbb{Q}_p} G_L.$$

In the case where V is de Rham, we can give an alternative formulation of its Hodge-Tate weights, using the filtration of $\mathbf{D}_{\mathrm{dR}}(V)$. Observe that an integer n is a Hodge-Tate weight of V if and only if $V\{-n\} = \mathrm{gr}^{-n}(\mathbf{D}_{\mathrm{HT}}(V)) \neq 0$. But by the preceding analysis, this is equivalent to

$$\mathrm{gr}^{-n}(\mathbf{D}_{\mathrm{dR}}(V)) = \mathrm{Fil}^{-n}\mathbf{D}_{\mathrm{dR}}(V)/\mathrm{Fil}^{-n+1}\mathbf{D}_{\mathrm{dR}}(V) \neq 0,$$

that is if we have a 'jump' in the filtration of $\mathbf{D}_{\mathrm{dR}}(V)$. Moreover the multiplicity of the Hodge-Tate weight n is given by the dimension of the quotient $\mathrm{Fil}^{-n}\mathbf{D}_{\mathrm{dR}}(V)/\mathrm{Fil}^{-n+1}\mathbf{D}_{\mathrm{dR}}(V)$. However, it's not always true that $\dim_L \mathbf{D}_{\mathrm{dR}}(V) = \dim_{L_0}\mathbf{D}_{\mathrm{cris}}(V)$, since there are representations which are de Rham but not crystalline.

Let us fix once and for all K to be the finite unramified extension of $\mathbb{Q}_p$ of degree f and denote by k its residue field $\mathbb{F}_q$, where $q = p^f$. Let also F be a finite extension of $\mathbb{Q}_p$ with residue field k_F. Write S for the set of $\mathbb{F}_p$-linear embeddings $\{k \hookrightarrow k_F\}$,which are in one to one correspondence with the $\mathbb{Q}_p$-linear embeddings $\{K \hookrightarrow F\}$ (we will be abusing notation to refer to embeddings $\{K \hookrightarrow F\}$ as elements of S). In particular we have that $\#S = [K : \mathbb{Q}_p]$. We also fix once and for all an embedding $\tau_0 \in S$ and write $\tau_i := \tau_0 \circ \mathrm{Frob}_p^i$. Then we get an identification of S with $\mathbb{Z}/f\mathbb{Z}$ via $\tau_i \mapsto i$. Now suppose V is an object of $\mathrm{Rep}_F^{\mathrm{cris}} G_K$. Then we have some finer variant of the Hodge-Tate weights of V. These are the labeled Hodge-Tate weights and are constructed as follows. We can consider the tensor $e_\tau \mathbf{D}_{\mathrm{cris}}(V) := \mathbf{D}_{\mathrm{cris}}(V) \bigotimes_{F \bigotimes_{\mathbb{Q}_p} K, \tau} F$, where F is given an $F \bigotimes_{\mathbb{Q}_p} K$-action via the map $(a \bigotimes b) \cdot x := a\tau(b)x$, for $a, x \in F$, $b \in K$. Then $e_\tau \mathbf{D}_{\mathrm{cris}}(V)$ can be thought of as an object of MF_F by giving it the filtration $\mathrm{Fil}^i e_\tau \mathbf{D}_{\mathrm{cris}}(V) := e_\tau \mathrm{Fil}^i \mathbf{D}_{\mathrm{cris}}(V) = \mathrm{Fil}^i \mathbf{D}_{\mathrm{cris}}(V) \bigotimes_{F \bigotimes_{\mathbb{Q}_p} K, \tau} F$. What we notice is that $\dim_F e_\tau \mathbf{D}_{\mathrm{cris}}(V) = \dim_{F \bigotimes_{\mathbb{Q}_p} K} \mathbf{D}_{\mathrm{cris}}(V) = \dim_F V$. Thus we define the ***labeled***

Hodge-Tate weights of V ***with respect to*** τ to be those integers n_τ for which $\mathrm{Fil}^{-n} e_\tau \mathbf{D}_{\mathrm{cris}}(V) \neq \mathrm{Fil}^{-n+1} e_\tau \mathbf{D}_{\mathrm{cris}}(V)$ and notice that we have $\dim_F V$ of them counted with multiplicity. The set of labeled Hodge-Tate weights of V with respect to all embeddings τ has cardinality $\#S \cdot \dim_F V$.

1.8 The theory of field of norms

In this section we give an overview of the construction of the field of norms for infinite, strictly APF extensions. We refer the reader to the paper of Wintenberger [28] for more information. So let us begin by fixing such an extension M/L that is also totally ramified. Let $\mathcal{E}_{M/L}$ denote the directed set of finite extensions of L contained in M, ordered by inclusion.

Definition 1.8.1. Define the field of norms of M/L by

$$X_L(M)^\times := \varprojlim_{E \in \mathcal{E}_{M/L}} E^\times,$$

where the transition maps are given by the norms $\mathrm{Nm}_{E'/E}$ whenever $E \subset E'$. Finally define

$$X_L(M) := X_L(M)^\times \cup \{0\}.$$

$X_L(M)$ is endowed with the following operations: Given $x, y \in X_L(M)$, $(xy)_E := x_E y_E$ and $(x+y)_E := \lim\limits_{E' \in \mathcal{E}_{M/L}} \mathrm{Nm}_{E'/E}(x_{E'} + y_{E'})$. Moreover, for any $E \in \mathcal{E}_{M/L}$ the valuation $v_E(x_E)$ is the same and so $X_L(M)$ is given the well defined discrete valuation $v(x) := v_E(x_E)$. Then one has that $X_L(M)$ is indeed a local field. Moreover, there exists an embedding $k_M \hookrightarrow X_L(M)$ which induces an isomorphism with the residue field of $X_L(M)$. Thus in particular $X_L(M)$ is an equicharacteristic local field (§2.1 of

[28]). If ϖ is a uniformizer of $X_L(M)$ then we have an isomorphism

$$X_L(M) \cong k_M((\varpi)).$$

If E/M is a finite Galois extension, then E/L is strictly APF. Now for any Galois extension N/M, we write

$$X_{M/L}(N) := \varinjlim_{E \in \mathcal{E}_{N/M}} X_L(E).$$

Notice that if $[N : M] < \infty$, then $X_{M/L}(N) = X_L(N)$.

Now let us suppose that the extension M/L is also totally ramified. If N/M is a Galois extension (not necessarily finite), we have that $\mathrm{Gal}(N/M)$ acts on $X_{M/L}(N)$. In particular, the action is given as follows. If N/M is a finite Galois extension, then $X_{M/L}(N)^\times = X_L(N)^\times = \varprojlim_{E \in \mathcal{E}_{N/L}} E^\times$. Given an element $\sigma \in \mathrm{Gal}(N/M)$ and $E \in \mathcal{E}_{N/L}$, there is a finite Galois extension of E stable under σ and contained in N. As a result, σ acts on the inverse limit $\varprojlim_{E \in \mathcal{E}_{N/L}} E^\times = X_L(N)^\times$. Moreover, one can show that this action is faithful (this is corollary 3.3.4 from [28]) and so we get an induced isomorphism

$$\mathrm{Gal}(N/M) \cong \mathrm{Gal}(X_L(N)/X_L(M)).$$

In the case where N/M is an infinite Galois extension, we have that

$$\begin{aligned} \mathrm{Gal}(X_{M/L}(N)/X_L(M)) &= \varprojlim_{E \in \mathcal{E}_{N/M}} \mathrm{Gal}(X_L(E)/X_L(M)) \\ &\cong \varprojlim_{E \in \mathcal{E}_{N/M}} \mathrm{Gal}(E/M) \\ &= \mathrm{Gal}(N/M). \end{aligned}$$

If X' is a separable (algebraic) extension of $X_L(M)$ then there exists an extension L' of M and an $X_L(M)$-isomorphism $X_L(L') \cong X'$. We thus have the following main theorem of the field of norms:

Theorem 1.8.2. *The category of (algebraic) extensions of M is equivalent to the category of (algebraic) separable extensions of $X_L(M)$, using the functor $X_{M/L}(.)$.*

This also implies that if $\overline{L}$ is an algebraic closure of L containing M, then $X_{M/L}(\overline{L})$ is a separable closure of $X_L(M)$ and

$$\mathrm{Gal}(\overline{M}/M) \cong \mathrm{Gal}(X_L(M)^{\mathrm{sep}}/X_L(M))$$

by identifying $\overline{M} = \overline{L}$ (§3.1, 3.2 of [28]).

Now let us restrict our attention to the p-adic cyclotomic tower $L_\infty := \bigcup_{n\geq 0} L(\zeta_{p^n})/L$. We let $\tilde{L}$ denote the unramified extension of L contained in L_∞. Then its Galois group $\Gamma_{\tilde{L}} = \mathrm{Gal}\ (L_\infty/\tilde{L})$ is isomorphic to to a finite index subgroup of $\mathbb{Z}_p^\times$ which is in turn a p-adic Lie group. It is a result of Sen [23] that totally ramified p-adic Lie extensions are strictly APF. Then in this case we put $X_L := X_{\tilde{L}}(L_\infty)$ and $\mathcal{O}_{X_L}$ for its valuation ring. Notice that X_L has an action of $\Gamma_{\tilde{L}}$. In the case where $L = \mathbb{Q}_p$, we write X for the separable closure of $X_{\mathbb{Q}_p}$, which is stable under the action of $G_{\mathbb{Q}_p}$. Then what we get is that $X_L = X^{H_L}$ and $H_L \cong \mathrm{Gal}(X/X_L) = G_{X_L}$, where $H_L = \mathrm{Gal}(\overline{L}/L_\infty)$. Recall from section 1.7, we had $\epsilon := (\zeta_{p^i})$ where ζ_{p^i} is a primitive p^i-th root of unity for all $i \geq 1$ and $\zeta_{p^0} = 1$. Then $\pi = \epsilon - 1$ is in fact a uniformizer for $X_{\mathbb{Q}_p}$ and thus $X_{\mathbb{Q}_p} \cong \mathbb{F}_p((\pi))$. Moreover, π has a Frobenius and $\Gamma_{\mathbb{Q}_p}$ action, given by

$$\phi(\pi) = (1+\pi)^p - 1 \text{ and } \gamma(\pi) = (1+\pi)^{\chi(\gamma)} - 1, \text{ for } \gamma \in \Gamma_{\mathbb{Q}_p}.$$

Let us now suppose $L/\mathbb{Q}_p$ is a finite extension. Later on we will need to be associating a field of norms to a finite extension M/L. The p-adic cyclotomic towers M_∞, L_∞ are infinite, strictly APF extensions of $\tilde{L}$ and $L_\infty/\tilde{L}$ is totally ramified. We associate to the extension M/L, the extension of the field of norms $X_{\tilde{L}}(M_\infty)/X_{\tilde{L}}(L_\infty)$. The theory of field of norms gives an isomorphism $\mathrm{Gal}(X_{\tilde{L}}(M_\infty)/X_{\tilde{L}}(L_\infty)) \cong \mathrm{Gal}(M_\infty/L_\infty)$.

Letting $L' := M \cap L_\infty$, we have

$$\begin{tikzcd}[column sep=small] & M_\infty \arrow[d, dash, "\mathrm{Gal}(M_\infty/L_\infty)\cong \mathrm{Gal}(X_{\tilde{L}}(M_\infty)/X_{\tilde{L}}(L_\infty))"] \\ M \arrow[ur, dash] \arrow[d, dash, "\mathrm{Gal}(M/L')"'] & L_\infty \\ L' \arrow[ur, dash] & \end{tikzcd}$$

So $\mathrm{Gal}(M_\infty/L_\infty) \cong \mathrm{Gal}(M/L')$. Moreover the quotient $\mathrm{Gal}(L'/L) \cong \mathrm{Gal}(M_\infty/L)/\mathrm{Gal}(M_\infty/L')$ is in fact a quotient of Γ_L. So we have

$$\begin{tikzcd} M \arrow[d, dash, "\mathrm{Gal}(M/L')\cong \mathrm{Gal}(X_{\tilde{L}}(M_\infty)/X_{\tilde{L}}(L_\infty))"] \\ L' \arrow[d, dash, "\mathrm{Gal}(L'/L)"] \\ L \end{tikzcd}$$

Recall from section 1.7, we defined the period ring $\tilde{\mathbb{E}}_L = \tilde{\mathbb{E}}^{H_L}$. Then there exists a continuous $G_{\tilde{L}}$-equivariant embedding (§4.2 of [28]),

$$\Lambda_{L_\infty/L} : X_L \hookrightarrow \tilde{\mathbb{E}}_L,$$

defined as follows. Let L_1 be the maximal tamely ramified subextension of $L_\infty/\tilde{L}$. Then for an integer n, put $q^E := [E : L_1]$ and

$$\mathcal{E}_n := \{E \subset L_\infty : E/L_1 \text{ is finite and } p^n | q^E\}.$$

Let $(x_n)_{n\in\mathbb{N}} \in X_L$ be some element and fix an integer m. Then define $y_m := \lim\limits_{n' \longrightarrow \infty} x_{n'}^{p^{-m}q^E}$, where the limit is taken over the subsequence $(x_{n'})_{n'} \in \mathcal{E}_m$. Finally, we define

$$\Lambda_{L_\infty/L}((x_n)_{n\in\mathbb{N}}) := (y_m)_{m\in\mathbb{N}}.$$

In particular, $\Lambda_{L_\infty/L}$ allows to identify X_L as a subfield of $\mathbb{E}_{\tilde{L}}$.

1.9 (ϕ, Γ)-modules in characteristic p

In this section we will introduce the category of (ϕ, Γ_L)-modules in characteristic p, which turns out to be equivalent to the category $\mathrm{Rep}_{\mathbb{F}_p} G_L$. This is possible due to the theory of field of norms. For more information, the reader is referred to Fontaine's paper [13]. Moreover, for the theory of (ϕ, Γ)-modules in characteristic p with extended coefficients the reader is referred to the paper of Chang-Diamond [7].

Recall the field $\mathbb{E}$ from the previous section which was defined as the separable closure of $\mathbb{E}_{\mathbb{Q}_p}$. We can also extend scalars for the period ring $\mathbb{E}$. To do that we define $\mathbb{E}_{L,F} := \mathbb{E}_L \bigotimes_{\mathbb{F}_p} k_F$ with Frobenius acting as $\phi \bigotimes 1$ and $\gamma \in \Gamma_L$ as $\gamma \bigotimes 1$. In the case where $L = K$, for K as always unramified, recall that we have that $\mathbb{E}_K \cong \mathbb{F}_q((\pi))$. Then we have that

$$\mathbb{E}_{K,F} = \mathbb{E}_K \bigotimes_{\mathbb{F}_p} k_F \cong \bigoplus_{\tau_i \in S} k((\pi)) \bigotimes_{k,\tau_i} k_F \cong \bigoplus_{\tau_i \in S} k_F((\pi)) = \bigoplus_{\tau_i \in S} \mathbb{E}_{\mathbb{Q}_p,F},$$

where the isomorphism is given by the projections $e_{\tau_i} : \alpha\pi^n \bigotimes \beta \mapsto (\tau_i(\alpha)\beta\pi^n)_{\tau_i \in S}$. The actions of ϕ and γ on $\bigoplus_{\tau_i \in S} \mathbb{E}_{\mathbb{Q}_p,F}$ then translate to

$$\phi(h_0(\pi), h_1(\pi), ..., h_{f-1}(\pi)) = (h_1(\phi(\pi)), h_2(\phi(\pi)), ..., h_{f-1}(\phi(\pi)), h_0(\phi(\pi)))$$

$$\gamma(h_0(\pi), h_1(\pi), ..., h_{f-1}(\pi)) = (h_0(\gamma(\pi)), h_1(\gamma(\pi)), ..., h_{f-1}(\gamma(\pi))).$$

So let us now define what a (ϕ, Γ_L)-module over $\mathbb{E}_{L,F}$ is.

Definition 1.9.1. A (ϕ, Γ_L)***-module over*** $\mathbb{E}_{L,F}$ is a finite rank module over $\mathbb{E}_{L,F}$ with a semilinear action of Frobenius ϕ and a continuous semilinear action of Γ_L, that commutes with the action of ϕ. Moreover, we say that a (ϕ, Γ_L)-module is ***étale*** if the span of the action of ϕ over $\mathbb{E}_{L,F}$, generates the whole module.

We remark that if a (ϕ, Γ_L)-module over $\mathbb{E}_{L,F}$ is étale then it is free. We write $\mathrm{Mod}^{\phi,\Gamma,\acute{e}t}_{\mathbb{E}_{L,F}}$ for the category of étale (ϕ, Γ_L)-modules of finite rank over $\mathbb{E}_{L,F}$. If M is an object of $\mathrm{Mod}^{\phi,\Gamma,\acute{e}t}_{\mathbb{E}_{K,F}}$, then we have that $M = \bigoplus_{\tau_i \in S} e_{\tau_i} M$. Then each $e_{\tau_i} M$ have ϕ and γ actions and the action of ϕ on M translates as $\phi \cdot M = \phi \cdot \bigoplus_{\tau_i \in S} e_{\tau_i} M = \bigoplus_{\tau_i \in S} e_{\tau_{i+1}} \phi \cdot M$. Thus each $e_{\tau_i} M$ is a (ϕ, Γ_K)-module over $\mathbb{E}_{\mathbb{Q}_p,F}$. The paper [7] contains the following classification result of rank one (ϕ, Γ_K)-modules over $\mathbb{E}_{K,F}$ (proposition 3.1 of [7]).

Proposition 1.9.2. *Let $\lambda_\gamma \in \mathbb{F}_p[[\pi]]$ be the unique $\frac{p^f-1}{p-1}$-th root of $\frac{\gamma(\pi)}{\overline{\chi}(\gamma)\pi}$, which is congruent to 1 mod π, if $\gamma \in \Gamma$ (recall $\overline{\chi}$ denotes the mod p cyclotomic character). For any $C \in k_F^\times$ and any $\vec{c} = (c_0, ..., c_{f-1}) \in \mathbb{Z}^S$, letting $M_{C,\vec{c}} = \mathbb{E}_{K,F} e$ with*

$$\phi(e) = Pe = (C\pi^{(p-1)c_0}, \pi^{(p-1)c_1}, ..., \pi^{(p-1)c_{f-1}})e,$$

$$\gamma(e) = G_\gamma e = (\lambda_\gamma^{\sum_0 \vec{c}}, \lambda_\gamma^{\sum_1 \vec{c}}, ..., \lambda_\gamma^{\sum_{f-1} \vec{c}})e,$$

where $\sum_l = \sum_l \vec{c} = \sum c_i p^j$ summing over $0 \le i, j \le f-1$, $i - j \equiv l$ mod f, defines an étale (ϕ, Γ_K)-module of rank one over $\mathbb{E}_{K,F}$. Conversely, for any rank one étale (ϕ, Γ_K)-module M over $\mathbb{E}_{K,F}$ we can choose a basis e so that $M = \mathbb{E}_{K,F} e$ with the action of ϕ and Γ given as above for some C and some $\vec{c}$. Two such modules M and M' are isomorphic if and only if $C = C'$ and $\sum_0 \vec{c} \equiv \sum_0 \vec{c'}$ mod $p^f - 1$. In particular, every rank one (ϕ, Γ_K)-module over $\mathbb{E}_{K,F}$ can be written uniquely in this form with $0 \le c_i \le p-1$ and at least one $c_i < p-1$.

We have a functor passing from the category $\mathrm{Rep}_{k_F} G_L$ to the category $\mathrm{Mod}^{\phi,\Gamma,\acute{e}t}_{\mathbb{E}_{L,F}}$;

$$\mathbf{D} : \mathrm{Rep}_{k_F} G_L \longrightarrow \mathrm{Mod}^{\phi,\Gamma,\acute{e}t}_{\mathbb{E}_{L,F}}$$

$$V \longmapsto (V \bigotimes_{\mathbb{F}_p} \mathbb{E})^{H_L}$$

$\mathbf{D}(V)$ inherits a ϕ-action from the action of ϕ on $\mathbb{E}$ and a $\Gamma_L = G_L/H_L$-action from the action of G_L on V. Hilbert's theorem 90 says that $\mathrm{H}^1(H_L, \mathrm{GL}_d(\mathbb{E})) = 0$ (where $d := \dim_{k_F} V$) and thus the tensor $V \bigotimes_{\mathbb{F}_p} \mathbb{E}$ with a semilinear action of H_L is isomorphic to $\mathbb{E}^d$. Hence $\mathbf{D}(V)$ has rank equal to d. Now if we have M some object of $\mathrm{Mod}_{\mathbb{E}_{K,F}}^{\phi,\Gamma,\acute{e}t}$ and give the tensor $M \bigotimes_{\mathbb{E}_K} \mathbb{E}$ a ϕ-action defined by $\phi_M \bigotimes \phi_{\mathbb{E}}$, then we get another functor;

$$\mathbf{V} : \mathrm{Mod}_{\mathbb{E}_{K,F}}^{\phi,\Gamma,\acute{e}t} \longrightarrow \mathrm{Rep}_{k_F} G_K$$

$$M \longmapsto (M \bigotimes_{\mathbb{E}_K} \mathbb{E})^{\phi=1}$$

where the G_K action on $\mathbf{V}(M)$ is given by the action of Γ_K on M and of $H_K \cong G_{\mathbb{E}_K}$ on $\mathbb{E}$. Notice that we have that $M \bigotimes_{\mathbb{E}_K} \mathbb{E} = (\bigoplus_{\tau_i \in S} e_{\tau_i} M) \bigotimes_{\mathbb{E}_K} \mathbb{E} = \bigoplus_{\tau_i \in S} (e_{\tau_i} M \bigotimes_{\mathbb{E}_K} \mathbb{E})$.

Theorem 1.9.3. *The functors* $\boldsymbol{D}$ *and* $\boldsymbol{V}$ *are quasi-inverses and the categories* $\mathrm{Mod}_{\mathbb{E}_{K,F}}^{\phi,\Gamma,\acute{e}t}$ *and* $\mathrm{Rep}_{k_F} G_K$ *are equivalent. Moreover, the two functors are exact, preserve dimensions and are compatible with tensor products.*

Proof. This is in the paper [13]. $\square$

Chapter 2

The Dembélé-Diamond-Roberts conjecture

In this chapter we give an overview of the weight part of Buzzard-Diamond-Jarvis [6] in the reducible case, as well as a statement of the Dembélé-Diamond-Roberts conjecture [8] in the strongly generic case. Recall that we write $K = \mathbb{Q}_{p^f}$, $q = p^f$ and S for the set of $\mathbb{F}_p$-linear embeddings $\{k \hookrightarrow \overline{\mathbb{F}}_p\}$ (where k is the residue field of K), which are in one to one correspondence with the $\mathbb{Q}_p$-linear embeddings $\{K \hookrightarrow \overline{\mathbb{Q}}_p\}$ (we will be sometimes abusing notation to refer to embeddings $\{K \hookrightarrow \overline{\mathbb{Q}}_p\}$ as elements of S). In particular we have that $\#S = [K : \mathbb{Q}_p] = f$. We also fix once and for all an embedding $\tau_0 \in S$ and write $\tau_i := \tau_0 \circ \mathrm{Frob}_p^i$. Then we get an identification of S with $\mathbb{Z}/f\mathbb{Z}$ via $\tau_i \mapsto i$. We also fix $-p$ as a uniformizer of K and drop the uniformizer subscript from the fundamental character defined on G_K.

2.1 The weight part of Buzzard-Diamond-Jarvis in the reducible case

A classification of irreducible $\overline{\mathbb{F}}_p$-representations of $\mathrm{GL}_2(k)$ is given by the following theorem.

Theorem 2.1.1. *Let V be an irreducible $\overline{\mathbb{F}}_p$-representations of $GL_2(k)$. Then V is equivalent to*

$$V_{\vec{a},\vec{b}} = \bigotimes_{\tau_i \in S} (det^{a_i} \bigotimes_{\mathbb{F}_q} Sym^{b_i-1}\mathbb{F}_q^2) \bigotimes_{\tau_i} \overline{\mathbb{F}}_p,$$

for some $a_i, b_i \in \mathbb{Z}$ satisfying $1 \leq b_i \leq p$, $0 \leq a_i \leq p-1$ for all $\tau_i \in S$ and $a_i < p-1$, for some τ_i. Thus there are $p^f(p^f-1)$ inequivalent irreducible representations.

Proof. See [1]. $\square$

Definition 2.1.2. We call an irreducible $\overline{\mathbb{F}}_p$-representation of $\mathrm{GL}_2(k)$ a ***Serre weight***.

Consider a reducible representation $\rho : G_K \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ of the form

$$\rho \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix} = \begin{pmatrix} \chi_1\chi_2^{-1} & c_\rho \\ 0 & 1 \end{pmatrix} \bigotimes \chi_2$$

Observe that c_ρ defines a cocycle in $\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$.

Next, in [6] the authors define the following set:

$$W'(\chi_1,\chi_2) := \left\{ (V_{\vec{a},\vec{b}}, J) \middle| J \subset S, \quad \chi_1 \mid_{I_K} = \prod_{i=0}^{f-1} \omega_{\tau_i,f}^{a_i} \prod_{j\in J} \omega_{\tau_j,f}^{b_j}, \quad \chi_2 \mid_{I_K} = \prod_{i=0}^{f-1} \omega_{\tau_i,f}^{a_i} \prod_{j\notin J} \omega_{\tau_j,f}^{b_j} \right\}$$

together with projections $\pi_1 : (V_{\vec{a},\vec{b}}, J) \mapsto V_{\vec{a},\vec{b}}$ and $\pi_2 : (V_{\vec{a},\vec{b}}, J) \mapsto J$. It's worth pointing out here that J is not unique and same $(\vec{a},\vec{b})$ can arise for different J. Let us fix some $\alpha := (V_{\vec{a},\vec{b}}, J) \in W'(\chi_1,\chi_2)$ and define $h_i := b_i$, if $i \in J$ and $h_i := -b_i$, if $i \notin J$.

Let $\psi := \chi_1\chi_2^{-1}$ which satisfies $\psi\mid_{\mathrm{I}_K}= \omega_{\tau_0,f}^{\sum_{i=0}^{f-1} h_ip^i}$. Lemma 3.9 of [6] guarantees the existence of a crystalline lift $\chi_\alpha : G_K \longrightarrow \overline{\mathbb{Q}}_p^\times$ of ψ with labeled Hodge-Tate weights $\vec{d} := (h_0, ..., h_{f-2}, h_{f-1})$. Moreover this lift is unique if we insist that if $g \in G_K^{\mathrm{ab}}$ corresponds to p via local class field theory, then $\chi_\alpha(g)$ is the Teichmüller lift of $\psi(g)$.

Let us now denote by $\mathrm{H}^1_f(G_K, \overline{\mathbb{Q}}_p(\chi_\alpha))$ (as defined by Bloch and Kato in [3]) the space of crystalline extensions

$$0 \longrightarrow \overline{\mathbb{Q}}_p(\chi_\alpha) \longrightarrow V \longrightarrow \overline{\mathbb{Q}}_p \longrightarrow 0$$

and consider the maps

$$\phi_1 : \mathrm{H}^1(G_K, \overline{\mathbb{Z}}_p(\chi_\alpha)) \longrightarrow \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$$

$$\phi_2 : \mathrm{H}^1(G_K, \overline{\mathbb{Z}}_p(\chi_\alpha)) \longrightarrow \mathrm{H}^1(G_K, \overline{\mathbb{Q}}_p(\chi_\alpha))$$

induced by reduction mod p and extension of scalars to $\overline{\mathbb{Q}}_p$ respectively. Put $L'_\alpha := \phi_1 \circ \phi_2^{-1}(\mathrm{H}^1_f(G_K, \overline{\mathbb{Q}}_p(\chi_\alpha)))$ and $L_\alpha := L'_\alpha$, except in the following cases:

- if ψ is cyclotomic, $J = S$ and $\vec{b} = \vec{p}$, we let $L_\alpha := \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$;
- if ψ is trivial and $J \neq S$, we let L_α be the span of L'_α and the unramified class L_{ur} (which is one dimensional).

We then have the following lemma:

Lemma 2.1.3. *If $\alpha = (V_{\vec{a},\vec{b}}, J) \in W'(\chi_1, \chi_2)$, then dim $L_\alpha = |J|$, except in the following cases:*

1. *if ψ is cyclotomic, $\vec{b} = \vec{p}$, $J = S$ and $p > 2$, then dim $L_\alpha = |J| + 1$;*
2. *if ψ is trivial, then dim $L_\alpha = |J| + 1$ unless either L_{ur} is not contained in L'_α or $\vec{b} = \vec{p}$, in which case dim $L_\alpha = |J| + 2$.*

Proof. This is lemma 3.12 in [6]. □

Finally, the authors of [6] define

$$W(\rho) := \{V : \exists J \subset S \text{ with } c_\rho \in L_\alpha \text{ for } \alpha = (V, J) \in W'(\chi_1, \chi_2)\}.$$

Then the conjecture 3.14 in [6] (now a theorem under technical hypothesis, see [15]), states that $W(\rho)$ is exactly the set of weights for which ρ is modular. Hence in order to describe explicitly the Serre weights for which ρ is modular, we need an explicit description of L_α. This contains precisely the reductions of the cocycles that can appear in lifts of $\rho \bigotimes \chi_2^{-1}$, which are crystalline with labeled Hodge-Tate weights $\{\vec{0}, \vec{d}\}$. If $\tilde{\rho}$ is such a lift, letting $\psi_2 : G_K \longrightarrow \overline{\mathbb{Q}}_p^\times$ be a crystalline lift of χ_2 with labeled Hodge-Tate weights $(a_{f-1}, a_0, ..., a_{f-2})$, we get that the twist $\tilde{\rho} \bigotimes \psi_2$ is indeed a crystalline lift of ρ (theorem 5.1.7 of [10]) with labeled Hodge-Tate weights $\{\vec{a}, \vec{a} + \vec{d}\}$. So we may write explicitly

$$L_\alpha = \left\{ c_\rho \in \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \,\middle|\, \begin{array}{c} \exists \tilde{c}_\rho \in \mathrm{H}^1(G_K, \overline{\mathbb{Q}}_p(\chi_\alpha)) \text{ such that } \tilde{c}_\rho \text{ reduces to } c_\rho \\ \text{and } \tilde{\rho} = \begin{pmatrix} \chi_\alpha & \tilde{c}_\rho \\ 0 & 1 \end{pmatrix} \text{ is crystalline.} \end{array} \right\},$$

apart from the case where ψ is cyclotomic or trivial, in which case L_α is bigger. In the paper [7], the authors give a description of the spaces L_α in terms of (ϕ, Γ) - modules. Moreover, the authors of the paper [8] have formulated a conjecture that gives an explicit description of L_α.

2.2 Statement of the conjecture in the strongly generic case

Let $(V_{\vec{a},\vec{b}}, J) \in W'(\chi_1, \chi_2)$, that is $\chi_1 \mid_{I_K} = \prod_{i=0}^{f-1} \omega_{\tau_i,f}^{a_i} \prod_{j \in J} \omega_{\tau_j,f}^{b_j}$ and $\chi_2 \mid_{I_K} = \prod_{i=0}^{f-1} \omega_{\tau_i,f}^{a_i} \prod_{j \notin J} \omega_{\tau_j,f}^{b_j}$, where $1 \leq b_i \leq p$, $0 \leq a_i \leq p-1$, and $J \subset S$. Recall we have defined in the previous section $h_i := \begin{cases} b_i, & \text{if } i \in J \\ -b_i & \text{if } i \notin J \end{cases}$. Notice that the congruence $\sum_{j=0}^{f-1} h_j p^j \equiv \sum_{j=0}^{f-1} c_j p^j \mod p^f - 1$ has a unique solution for $1 \leq c_j \leq p$ unless $\psi|_{I_K} = \chi_1 \chi_2^{-1}|_{I_K}$ is the mod p cyclotomic character, in which case we can take all c_j to be equal to 1 or p. Put $c := \sum_{i=0}^{f-1} c_i p^i$. Then we have that

$$\chi_1 \chi_2^{-1}|_{I_K} = \prod_{i \in J} \omega_{\tau_i,f}^{b_i} \prod_{i \notin J} \omega_{\tau_i,f}^{-b_i} = \prod_{i \in S} \omega_{\tau_i,f}^{h_i} = \omega_{\tau_0,f}^{c}.$$

Note that J is not necessarily unique for fixed $(\vec{a}, \vec{b})$. That is, if $V_{\vec{a},\vec{b}} \in W(\rho)$, then there might be more than one $J \subset S$ such that $\alpha := (V_{\vec{a},\vec{b}}, J) \in W'(\chi_1, \chi_2)$ and $c_\rho \in L_\alpha$. However, in the case where $1 \leq b_i \leq p-1$, it is clear that we do have uniqueness of J. In the paper [15] the authors prove the following:

Theorem 2.2.1. *Let $V = V_{\vec{a},\vec{b}}$ be a Serre weight in $W(\rho)$. Then there exists a unique $J = J_{max}(V)$ with $c_\rho \in L_\alpha$, for $\alpha = (V, J) \in W'(\chi_1, \chi_2)$, satisfying the following conditions:*

1. *if $(b_j, b_{j+1}, ..., b_i) = (p, p-1, ..., p-1, 1)$ with $j, j+1, ..., i-1 \notin J$, then $i \notin J$;*
2. *if $\vec{b} = p \vec{-} 1$, then J is non-empty.*

Proof. This is in section 8.2 of [15]. ∎

As a result we get a well defined map

$$\phi : W(\rho) \longrightarrow \{J : J \subset S\}$$

$$V \longmapsto J_{\max}(V).$$

Moreover we have the following lemma:

Lemma 2.2.2. *Specifying $J \subset S$, we can always find $\vec{m}$, $\vec{n}$ with $1 \leq n_i, m_i \leq p$ for all i such that*

$$\sum_{i=0}^{f-1} c_i p^i \equiv \sum_{i \in J} m_i p^i - \sum_{i \notin J} n_i p^i \quad mod\ p^f - 1,$$

satisfying the above conditions. The congruence has a unique solution, unless $m_i = p$ for $i \in J$ and $n_i = 1$ for $i \notin J$, or $m_i = 1$ for $i \in J$ and $n_i = p$ for $i \notin J$. In this case the congruence has two solutions.

Proof. See [6] section §5.1. $\square$

Definition 2.2.3. Let $\psi = \mathrm{unr}_x \omega_{\tau_0,f}^{\sum_{i=0}^{f-1} c_i p^i} : G_K \longrightarrow \overline{\mathbb{F}}_p^{\times}$. We say that ψ is ***strongly generic*** when

- $1 \leq c_i \leq p-2$ for $0 \leq i \leq f-1$;
- $\mathrm{hcf}(c, p^f - 1) = 1$;
- $\mathrm{unr}_x = 1$.

Lemma 2.2.4. *A strongly generic character is primitive.*

Proof. The only property that we need from strong genericity is that $\mathrm{hcf}(c, p^f - 1) = 1$. Notice that if we suppose that the character is not primitive then c has a non-trivial stabilizer under the action of $\mathrm{Gal}(k_L/\mathbb{F}_p)$ that we defined in section 1.6. Hence there exists a natural number $n < f$ that divides f such that $c \equiv p^n c \mod p^f - 1$. But then there exists some integer a such that $c(p^n - 1) = (p^f - 1)a$. Since n divides f, $\frac{p^f-1}{p^n-1}$ is an integer that divides both c and $p^f - 1$, which is a contradiction. $\square$

If ψ is of the form $\chi_1\chi_2^{-1}$ and strongly generic, fixing $J \subset S$ uniquely determines $\chi_1 \mid_{I_K}$ and $\chi_2 \mid_{I_K}$. We let $\vec{v_1} := \begin{cases} p, & \text{if } i \in J \\ 1, & \text{if } i \notin J \end{cases}$ and $\vec{v_2} := \begin{cases} 1, & \text{if } i \in J \\ p, & \text{if } i \notin J \end{cases}$. We define the set of exceptional Serre weights

$$W_{\text{excep.}}(\rho) := W(\rho) \cap \{V_{\vec{a},\vec{a}+v_1}, V_{\vec{a},\vec{a}+v_2} : 0 \leq a \leq p-1\}.$$

In the same fashion we can also define a set of exceptional $J's$ as follows.

$$J_{\text{excep.}}(\rho) := \{J \subset S | \text{ for } V \in W_{\text{excep.}}(\rho) \text{ and } \alpha = (V, J) \in W'(\chi_1, \chi_2), c_\rho \in L_\alpha\}.$$

Then we get that the map

$$\phi : W(\rho) \setminus W_{\text{excep.}}(\rho) \longrightarrow \{J : J \subset S\} \setminus J_{\text{excep.}}(\rho)$$

$$V \longmapsto J_{\max}(V)$$

is injective. Let us write $G := \mathrm{Gal}(L'/L)$, where L'/L is not necessarily finite and $\mathbb{Q}_p \subset L$. Let also $\chi : G \longrightarrow \overline{\mathbb{F}}_p$ be a character. In the paper [8], the authors define two increasing filtrations on $\mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi))$ as follows.

Definition 2.2.5. Let $s \in [0, \infty) \cap \mathbb{R}$. We define

$$\mathrm{Fil}^s\mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) := \bigcap_{v > s-1} \ker(\mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) \longrightarrow \mathrm{H}^1(G^v, \overline{\mathbb{F}}_p(\chi))).$$

We extend the filtration to the whole of $\mathbb{R}$ by setting $\mathrm{Fil}^s\mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) := 0$, for $s < 0$. The second filtration is defined as

$$\mathrm{Fil}^{<t}\mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) := \bigcup_{s<t} \mathrm{Fil}^s\mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)),$$

for $t \in \mathbb{R}$. Notice that in the case where G is finite, we have that the function $s \mapsto \dim_{\overline{\mathbb{F}}_p} \mathrm{Fil}^s \mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi))$ is locally constant on intervals $[s, s')$, where $\Psi(s) \in \mathbb{Z}$ and $\Psi(s') = \Psi(s) + 1$. So it follows that the function is also upper semi-continuous. In particular since $\Psi(u) = u$ for $0 \leq u < 1$, we have that

$$\mathrm{Fil}^s \mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) = \mathrm{Fil}^0 \mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) = \ker(\mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) \longrightarrow \mathrm{H}^1(I(L'/L), \overline{\mathbb{F}}_p(\chi))),$$

for $0 \leq s < 1$.

We now assume that G is no longer finite. Recall that we had that $G^u = I_L$, for $-1 < u \leq 0$. So it still holds that

$$\mathrm{Fil}^s \mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) = \mathrm{Fil}^0 \mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) = \ker(\mathrm{H}^1(G, \overline{\mathbb{F}}_p(\chi)) \longrightarrow \mathrm{H}^1(I_L, \overline{\mathbb{F}}_p(\chi))),$$

for $0 \leq s < 1$. From now on we restrict our attention to the case where $G = G_K$ and $\chi = \psi = \chi_1 \chi_2^{-1}$. Then we have the following proposition.

Proposition 2.2.6.

$$\mathit{Fil}^{<s} H^1(G_K, \overline{\mathbb{F}}_p(\psi)) = \mathit{ker}(H^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow H^1(G_K^{s-1}, \overline{\mathbb{F}}_p(\psi))).$$

Proof. Using the fact that for $u \leq v$,

$$\ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(G_K^u, \overline{\mathbb{F}}_p(\psi))) \subset \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(G_K^v, \overline{\mathbb{F}}_p(\psi))),$$

we have that

$$\mathrm{Fil}^{<s} \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \quad \subset \quad \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(G_K^{s-1}, \overline{\mathbb{F}}_p(\psi))).$$

Conversely, if $s < 0$ we have that $\mathrm{Fil}^{<s} \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) = 0$, since $\mathrm{Fil}^s \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) = 0$ for $s < 0$. For $0 < s < 1$, we have that $\mathrm{Fil}^s \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) = \mathrm{Fil}^0 \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) = \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(I_K, \overline{\mathbb{F}}_p(\psi)))$. So we get that for $0 < s \leq 1$,

$$\mathrm{Fil}^{<s} \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) = \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(I_K, \overline{\mathbb{F}}_p(\psi))).$$

Thus it remains to show the case for $s > 1$. Let $\alpha \in \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(G_K^{s-1}, \overline{\mathbb{F}}_p(\psi))$. Then we need to show that there exists some $\epsilon > 0$ such that $\alpha \in \mathrm{Fil}^{s-\epsilon}\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$. Equivalently since $\mathrm{Fil}^s\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$ is increasing with respect to s, it suffices to find an ϵ such that α restricted to $G_K^{s-1-\epsilon}$ is trivial. We have that α satisfies the cocycle condition $\alpha(gh) = \alpha(g) + \psi(g)\alpha(h)$. Since $\psi \mid_{I_K}$ factors through a tamely ramified quotient of I_K (see lemma 1.6.5), we have that α restricted to wild inertia P_K is a homomorphism $P_K \longrightarrow \overline{\mathbb{F}}_p$, since ψ is trivial. Since K is a local field, we have that the cohomology group $\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$ is finite dimensional over $\overline{\mathbb{F}}_p$. So let's suppose $\psi_1, ..., \psi_m$ are the basis elements. We have that each $\psi_i \mid_{P_K}$ is a group homomorphism with open kernel H_i. Letting $H := \cap_{i=1}^m H_i$ we have an open subgroup of P_K, and hence of finite index. Letting G to be the quotient, we get that G is finite.

So if $\alpha \mid_{G_K^{s-1}}$ is trivial, then it is also trivial on $G_K^{s-1}H/H = (P_K/H)^{s-1} = G^{s-1}$ (recall that $G_K^{s-1} \subseteq P_K$ and using proposition 1.1.4). But G is finite and so $G^{s-1} = G_{\lceil \Psi(s-1) \rceil}$ and since the ceiling function is lower semi-continuous, we can find an $\epsilon > 0$ such that $G^{s-1} = G^{s-1-\epsilon} = G_K^{s-1-\epsilon}H/H$. Thus α is trivial on $G_K^{s-1-\epsilon}$ and finishes the proof. $\square$

Next we highlight certain subspaces in the filtration that are going to play an important role.

Definition 2.2.7. We define the following subspaces of $\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$;

1. $\mathrm{H}^1_{\mathrm{ur}}(G_K, \overline{\mathbb{F}}_p(\psi)) := \mathrm{Fil}^0\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$, the ***unramified subspace*** of $\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$;

2. $\mathrm{H}^1_{\mathrm{gt}}(G_K, \overline{\mathbb{F}}_p(\psi)) := \mathrm{Fil}^{<\frac{p}{p-1}}\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$, the ***gently ramified*** subspace of $\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$;

3. $\mathrm{H}^1_{\mathrm{ty}}(G_K, \overline{\mathbb{F}}_p(\psi)) := \mathrm{Fil}^{<1+\frac{p}{p-1}}\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$, the ***typically ramified*** subspace of $\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$.

So using the previous proposition we have that

$$\mathrm{H}^1_{\mathrm{ur}}(G_K, \overline{\mathbb{F}}_p(\psi)) = \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(I_K, \overline{\mathbb{F}}_p(\psi)));$$

$$\mathrm{H}^1_{\mathrm{gt}}(G_K, \overline{\mathbb{F}}_p(\psi)) = \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(G_K^{\frac{1}{p-1}}, \overline{\mathbb{F}}_p(\psi)));$$

$$\mathrm{H}^1_{\mathrm{ty}}(G_K, \overline{\mathbb{F}}_p(\psi)) = \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(G_K^{\frac{p}{p-1}}, \overline{\mathbb{F}}_p(\psi)))$$

and

$$\mathrm{H}^1_{\mathrm{ur}}(G_K, \overline{\mathbb{F}}_p(\psi)) \quad \subset \quad \mathrm{H}^1_{\mathrm{gt}}(G_K, \overline{\mathbb{F}}_p(\psi)) \quad \subset \quad \mathrm{H}^1_{\mathrm{ty}}(G_K, \overline{\mathbb{F}}_p(\psi)).$$

Notice that the inflation-restriction exact sequence

$$0 \longrightarrow \mathrm{H}^1(G_k, \overline{\mathbb{F}}_p(\psi)^{I_K}) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(I_K, \overline{\mathbb{F}}_p(\psi))^{G_k} \longrightarrow \dots$$

gives an isomorphism $\mathrm{H}^1_{\mathrm{ur}}(G_K, \overline{\mathbb{F}}_p(\psi)) \cong \mathrm{H}^1(G_k, \overline{\mathbb{F}}_p(\psi)^{I_K})$. These subspaces also satisfy the following properties:

Proposition 2.2.8. *1. $H^1_{ur}(G_K, \overline{\mathbb{F}}_p(\psi)) = 0$ unless ψ is trivial, in which case $dim_{\overline{\mathbb{F}}_p} H^1_{ur}(G_K, \overline{\mathbb{F}}_p(\psi)) = 1$;*

2. $H^1(G_K, \overline{\mathbb{F}}_p(\psi)) = H^1_{ty}(G_K, \overline{\mathbb{F}}_p(\psi))$ unless ψ is cyclotomic, in which case $dim_{\overline{\mathbb{F}}_p} H^1(G_K, \overline{\mathbb{F}}_p(\psi))/H^1_{ty}(G_K, \overline{\mathbb{F}}_p(\psi)) = 1$;

3. $dim_{\overline{\mathbb{F}}_p} H^1_{ty}(G_K, \overline{\mathbb{F}}_p(\psi))/H^1_{ur}(G_K, \overline{\mathbb{F}}_p(\psi)) = f$;

4. $dim_{\overline{\mathbb{F}}_p} H^1_{gt}(G_K, \overline{\mathbb{F}}_p(\psi))/H^1_{ur}(G_K, \overline{\mathbb{F}}_p(\psi))$ is equal to the number of elements of the set $S' := \{i \in S | c_i = p\}$.

Proof. This is corollary 3.2 in [8]. $\square$

Corollary 2.2.9. *Let $s' := \#S'$. Then*

$$dim_{\overline{\mathbb{F}}_p} H^1_{ty}(G_K, \overline{\mathbb{F}}_p(\psi))/H^1_{gt}(G_K, \overline{\mathbb{F}}_p(\psi)) = f - s'.$$

Writing $G := \mathrm{Gal}(L/K)$, the inflation-restriction exact sequence

$$0 \longrightarrow \mathrm{H}^1(G, \overline{\mathbb{F}}_p(\psi)^{G_L}) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(G_L, \overline{\mathbb{F}}_p(\psi))^G \longrightarrow \mathrm{H}^2(G, \overline{\mathbb{F}}_p(\psi)^{G_L}) \longrightarrow \dots$$

gives an isomorphism $\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \cong \mathrm{H}^1(G_L, \overline{\mathbb{F}}_p(\psi))^G$, since $\mathrm{H}^i(G, \overline{\mathbb{F}}_p(\psi)^{G_L}) = 0$, for all $i > 0$ (the order of G is prime to p).

What we observe next is that $\mathrm{H}^1(G_L, \overline{\mathbb{F}}_p(\psi))^G \cong \mathrm{Hom}_{\mathbb{F}_p[G]}(G_L, \overline{\mathbb{F}}_p(\psi)) = \mathrm{Hom}_{\mathbb{F}_p[G]}(G_L^{\mathrm{ab}}, \overline{\mathbb{F}}_p(\psi))$. By continuity, each homomorphism $G_L^{\mathrm{ab}} \longrightarrow \overline{\mathbb{F}}_p(\psi)$ factors through a finite quotient of G_L^{ab} and so through a finite quotient of W_L^{ab}. Thus $\mathrm{Hom}_{\mathbb{F}_p[G]}(G_L^{\mathrm{ab}}, \overline{\mathbb{F}}_p(\psi)) = \mathrm{Hom}_{\mathbb{F}_p[G]}(W_L^{\mathrm{ab}}, \overline{\mathbb{F}}_p(\psi))$ and by class field theory, $\mathrm{Hom}_{\mathbb{F}_p[G]}(W_L^{\mathrm{ab}}, \overline{\mathbb{F}}_p(\psi)) \cong \mathrm{Hom}_{\mathbb{F}_p[G]}(L^\times, \overline{\mathbb{F}}_p(\psi))$, the isomorphism being given by precomposing with Art_L. Moreover, since the image of an element of $\mathrm{Hom}_{\mathbb{F}_p[G]}(L^\times, \overline{\mathbb{F}}_p(\psi))$ is killed by p, we also have that $\mathrm{Hom}_{\mathbb{F}_p[G]}(L^\times, \overline{\mathbb{F}}_p(\psi)) = \mathrm{Hom}_{\mathbb{F}_p[G]}(L^\times/(L^\times)^p, \overline{\mathbb{F}}_p(\psi))$. Hence we conclude that

Lemma 2.2.10.

$$H^1(G_K, \overline{\mathbb{F}}_p(\psi)) \cong Hom_{\mathbb{F}_p[G]}(L^\times/(L^\times)^p, \overline{\mathbb{F}}_p(\psi)).$$

We can play the same game with the following exact sequence.

$$0 \longrightarrow \mathrm{H}^1(\mathrm{Gal}(k_L/k), \overline{\mathbb{F}}_p(\psi)^{I_L}) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G_k, \overline{\mathbb{F}}_p(\psi)) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(G_{k_L}, \overline{\mathbb{F}}_p(\psi))^{\mathrm{Gal}(k_L/k)} \longrightarrow \mathrm{H}^2(\mathrm{Gal}(k_L/k), \overline{\mathbb{F}}_p(\psi)^{I_L}) \longrightarrow \dots$$

We have again that $\mathrm{H}^i(\mathrm{Gal}(k_L/k), \overline{\mathbb{F}}_p(\psi)^{I_L}) = 0$, for all $i > 0$, since $\#\mathrm{Gal}(k_L/k) = r$ which is prime to p. So we get an isomorphism

$$\begin{aligned} \mathrm{H}^1_{\mathrm{ur}}(G_K, \overline{\mathbb{F}}_p(\psi)) &\cong \mathrm{H}^1(G_{k_L}, \overline{\mathbb{F}}_p(\psi))^{\mathrm{Gal}(k_L/k)} \\ &= \mathrm{Hom}_{\mathbb{F}_p[\mathrm{Gal}(k_L/k)]}(G_{k_L}, \overline{\mathbb{F}}_p(\psi)) \\ &= \mathrm{Hom}_{\mathbb{F}_p[G]}(\mathbb{Z}/p\mathbb{Z}, \overline{\mathbb{F}}_p(\psi)). \end{aligned}$$

Lemma 2.2.11.

$$H^1(G_K, \overline{\mathbb{F}}_p(\psi))/H^1_{ur}(G_K, \overline{\mathbb{F}}_p(\psi)) \cong Hom_{\mathbb{F}_p[G]}(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p, \overline{\mathbb{F}}_p(\psi)).$$

Proof. The short exact sequence

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0$$

is split by the choice of a uniformizer, so reducing mod p and applying the functor $\mathrm{Hom}_{\mathbb{F}_p[G]}(\_, \overline{\mathbb{F}}_p(\psi))$, the sequences

$$1 \longrightarrow \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \longrightarrow L^\times/(L^\times)^p \xrightarrow{v_L} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

and

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_{\mathbb{F}_p[G]}(\mathbb{Z}/p\mathbb{Z}, \overline{\mathbb{F}}_p(\psi)) &\longrightarrow \mathrm{Hom}_{\mathbb{F}_p[G]}(L^\times/(L^\times)^p, \overline{\mathbb{F}}_p(\psi)) \\ \longrightarrow \mathrm{Hom}_{\mathbb{F}_p[G]}(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p, \overline{\mathbb{F}}_p(\psi)) &\longrightarrow 0 \end{aligned}$$

are still exact. $\square$

L/K is tamely ramified and thus $P_L = P_K$ and $G_K^u \subset G_L$, for all $u > 0$. This allows us to write $G_K^u = \varprojlim_{K'/K} \mathrm{Gal}(K'/K)_{\Psi_{K'/K}(u)} = \varprojlim_{K'/L} \mathrm{Gal}(K'/L)_{\Psi_{K'/K}(u)}$. We also have that $\mathrm{Gal}(L/K)_u = 0$ for all $u \geq 1$ and $[\mathrm{Gal}(L/K)_0 : \mathrm{Gal}(L/K)_t] =$

$\#I(L/K) = e$ for all $t > 0$. Thus $\Phi_{L/K}(ue) = \int_0^{ue}[\mathrm{Gal}(L/K)_0 : \mathrm{Gal}(L/K)_t]^{-1}dt = \int_0^{ue}(\#I(L/K))^{-1}dt = u$. Hence $\Psi_{L/K}(u) = ue$ and using proposition 1.1.3, $\Psi_{K'/K}(u) = \Psi_{K'/L} \circ \Psi_{L/K}(u) = \Psi_{K'/L}(ue)$. So

$$G_K^u = \varprojlim_{K'/L} \mathrm{Gal}(K'/L)_{\Psi_{K'/L}(ue)} = G_L^{ue}.$$

Recall that we defined in section 1.4 the unit groups

$$U_L^i = \ker(\mathcal{O}_L^\times \xrightarrow[\text{mod } \pi_L^i]{} (\mathcal{O}_L/\pi_L^i\mathcal{O}_L)^\times) \cong 1 + \pi_L^i\mathcal{O}_L .$$

These define a decreasing filtration of G-modules

$$\mathcal{O}_L^\times = U_L^0 \supset U_L^1 \supset U_L^2 \supset \cdots$$

and satisfy the following:

$$U_L^0/U_L^1 \cong k_L^\times \text{ and for } i \geq 1,\ U_L^i/U_L^{i+1} \cong (k_L, +).$$

Lemma 2.2.12. *Let us abbreviate $H^1_{ty}(G_K, \overline{\mathbb{F}}_p(\psi))$ by H^1_{ty} and similarly $H^1_{gt}(G_K, \overline{\mathbb{F}}_p(\psi))$ by H^1_{gt}. Then we have*

$$H^1_{gt} \cong Hom_{\mathbb{F}_p[G]}(L^\times/(L^\times)^p U_L^{\frac{e}{p-1}}, \overline{\mathbb{F}}_p(\psi));$$

$$H^1_{ty} \cong Hom_{\mathbb{F}_p[G]}(L^\times/(L^\times)^p U_L^{\frac{pe}{p-1}}, \overline{\mathbb{F}}_p(\psi)).$$

Proof. If $u > 0$, then $(G_L^{\mathrm{ab}})^u \subset I_L^{\mathrm{ab}} \subset W_L^{\mathrm{ab}}$ and using corollary 3 of chapter XV of [24], we have

$$\mathrm{Art}_L^{-1}|_{(G_L^{\mathrm{ab}})^u} \twoheadrightarrow U_L^{\lceil u \rceil} .$$

So using $(G_K^{\mathrm{ab}})^u = (G_L^{\mathrm{ab}})^{ue}$ we have that for

$$\alpha \in \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \cong \mathrm{H}^1(G_L, \overline{\mathbb{F}}_p(\psi))^G \cong \mathrm{Hom}_{\mathbb{F}_p[G]}(W_L^{\mathrm{ab}}, \overline{\mathbb{F}}_p(\psi)),$$

$$\alpha \in \ker(\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{H}^1(G_K^u, \overline{\mathbb{F}}_p(\psi))) \iff (L^\times)^p U_L^{ue} \subset \ker(\alpha \circ \mathrm{Art}_L).$$

□

Corollary 2.2.13. *Suppose we are in the strongly generic case and let* $t := \frac{e}{p-1} = \frac{p^f-1}{p-1}$. *Then we have that*

$$H^1_{ty}/H^1_{gt} \cong Hom_{\mathbb{F}_p[G]}(U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t, \overline{\mathbb{F}}_p(\psi)).$$

Proof. The exact sequence

$$1 \longrightarrow U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t \longrightarrow L^\times/(L^\times)^p U_L^{t+e} \longrightarrow L^\times/(L^\times)^p U_L^t \longrightarrow 1$$

is split, since $p \nmid |G|$. So the following sequence is also exact

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{F}_p[G]}(L^\times/(L^\times)^p U_L^t, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{Hom}_{\mathbb{F}_p[G]}(L^\times/(L^\times)^p U_L^{t+e}, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{Hom}_{\mathbb{F}_p[G]}(U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t, \overline{\mathbb{F}}_p(\psi)) \longrightarrow 0$$

□

Definition 2.2.14. Suppose we are in the strongly generic case and let $i \notin J$. Then define

$$s_i := \sum_{j=0}^{f-1} c_{i+j+1} p^j.$$

For the rest of this section, we assume we are in the strongly generic case. In this case we have that $\mathrm{H}^1_{\mathrm{gt}} = 0$ and $\mathrm{H}^1_{\mathrm{ty}} = \mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi))$. Hence by corollary 2.2.13 we have that

Corollary 2.2.15.

$$H^1(G_K, \overline{\mathbb{F}}_p(\psi)) \cong Hom_{\mathbb{F}_p[G]}(U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t, \overline{\mathbb{F}}_p(\psi)).$$

Notice that by lemma 2.2.4 we have that the integers s_i, for $i \in J$, are distinct. We also have that $k_L = k$, $\psi = \omega^c_{\tau_0,f}$. Since L is the splitting field of ψ and in the strongly generic case $\mathrm{hcf}(c, p^f - 1) = 1$, we have the following lemma.

Lemma 2.2.16.

$$L = K(\sqrt[p^f-1]{-p})$$

Lemma 2.2.17. *The Artin-Hasse exponential E_p is multiplicative on $\pi_L^t\mathcal{O}_L/\pi_L^{t+e}\mathcal{O}_L$ and it induces an isomorphism $\pi_L^t\mathcal{O}_L/\pi_L^{t+e}\mathcal{O}_L \cong U_L^t/U_L^{t+e}$. In particular, E_p is given on this quotient by $E_p(x) = \sum_{n=0}^{p-1} \frac{x^n}{n!}$.*

Proof. Recall that in the strongly generic case $t = \frac{p^f-1}{p-1}$ and so $pt = t + e$. Moreover, $|\cup \mathrm{Syl}_p(S_n)| = 1$ for $n < p$ and so by theorem 1.4.2, we get the result. $\square$

Notice that the integers s_i are contained in the range $[t, t + e)$. In particular we get an injection

$$k\pi_L^{s_i} \hookrightarrow \pi_L^t\mathcal{O}_L/\pi_L^{t+e}\mathcal{O}_L \xrightarrow[E_p]{\sim} U_L^t/U_L^{t+e} \twoheadrightarrow U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t$$

Lemma 2.2.18. *In the strongly generic case $\{E_p(\pi_L^{s_j})$ mod $U_L^{t+e}(L^\times)^p \cap U_L^t : 0 \leq j \leq f-1\}$ are linearly independent as elements of $U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t$.*

Proof. We first notice that $\{\pi_L^{s_j} : 0 \leq j \leq f-1\}$ are linearly independent as elements of $\pi_L^t\mathcal{O}_L/\pi_L^{t+e}\mathcal{O}_L$. Thus we have that $\{E_p(\pi_L^{s_j}) : 0 \leq j \leq f-1\}$ are linearly independent as elements of U_L^t/U_L^{t+e}. Let $x \in \pi_L^t\mathcal{O}_L/\pi_L^{t+e}\mathcal{O}_L$ and consider $E_p(x)^p = E_p(px)$. Then we have that $v_L(px) \geq p^f - 1 + t = pt$ and $px \equiv 0 \bmod \pi_L^{t+e}$. $\square$

We would like to remark here that the elements $\{E_p(\pi_L^{s_j}) : 0 \leq j \leq f-1\}$ form part of what is known as the Shafarevich basis of U_L^1 (see [9] Chapter VI, proposition 5.2).

The previous injection sits in an exact sequence

$$0 \longrightarrow k\pi_L^{s_i} \longrightarrow U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t \longrightarrow A \longrightarrow 0\ .$$

Applying $\mathrm{Hom}_{\mathbb{F}_p}(\_, \overline{\mathbb{F}}_p(\psi))$ to this exact sequence we get

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{F}_p}(A, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{Hom}_{\mathbb{F}_p}(U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t, \overline{\mathbb{F}}_p(\psi)) \longrightarrow \mathrm{Hom}_{\mathbb{F}_p}(k\pi_L^{s_i}, \overline{\mathbb{F}}_p(\psi))\ .$$

and taking G-invariants we get

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{H}^0(G, \mathrm{Hom}_{\mathbb{F}_p}(A, \overline{\mathbb{F}}_p(\psi))) \arrow[r] & \mathrm{H}^0(G, \mathrm{Hom}_{\mathbb{F}_p}(U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t, \overline{\mathbb{F}}_p(\psi))) \arrow[dll, rounded corners] \\ \mathrm{H}^0(G, \mathrm{Hom}_{\mathbb{F}_p}(k\pi_L^{s_i}, \overline{\mathbb{F}}_p(\psi))) \arrow[r] & \mathrm{H}^1(G, \mathrm{Hom}_{\mathbb{F}_p}(A, \overline{\mathbb{F}}_p(\psi))) \arrow[r] & \ldots \end{tikzcd}$$

However, the order of the group G is prime to p and we have that

$$\mathrm{H}^1(G, \mathrm{Hom}_{\mathbb{F}_p}(A, \overline{\mathbb{F}}_p(\psi))) = 0.$$

Also,

$$\mathrm{H}^0(G, \mathrm{Hom}_{\mathbb{F}_p}(U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t, \overline{\mathbb{F}}_p(\psi))) = \mathrm{Hom}_{\mathbb{F}_p[G]}(U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t, \overline{\mathbb{F}}_p(\psi))$$

and

$$\mathrm{H}^0(G, \mathrm{Hom}_{\mathbb{F}_p}(k\pi_L^{s_i}, \overline{\mathbb{F}}_p(\psi))) = \mathrm{Hom}_{\mathbb{F}_p[G]}(k\pi_L^{s_i}, \overline{\mathbb{F}}_p(\psi)).$$

Therefore, we get a surjection

$$\mathrm{Hom}_{\mathbb{F}_p[G]}(U_L^t/U_L^{t+e}(L^\times)^p \cap U_L^t, \overline{\mathbb{F}}_p(\psi)) \twoheadrightarrow \mathrm{Hom}_{\overline{\mathbb{F}}_p[G]}(k\pi_L^{s_i} \bigotimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p, \overline{\mathbb{F}}_p(\psi))\ .$$

The extension L/K is a Kummer extension and so G_K acts on L via the character $\omega^{\frac{p^f-1}{e}} : G_K \longrightarrow L$, $\omega^{\frac{p^f-1}{e}}(g) := (\frac{g(\sqrt[p^f-1]{-p})}{\sqrt[p^f-1]{-p}})^{\frac{p^f-1}{e}} = \frac{g(\sqrt[e]{-p})}{\sqrt[e]{-p}} = \frac{g\cdot\pi_L}{\pi_L}$. In particular, $k\pi_L^{s_i}$ as a G-module is isomorphic to $k(\omega^{s_i})$. Thus the above surjection becomes

$$\mathrm{H}^1(G_K, \overline{\mathbb{F}}_p(\psi)) \twoheadrightarrow \mathrm{Hom}_{\overline{\mathbb{F}}_p[G]}(k(\omega^{s_i}) \bigotimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p, \overline{\mathbb{F}}_p(\psi))\ .$$

We also have an isomorphism

$$k(\omega^{s_i})\bigotimes_{\mathbb{F}_p}\overline{\mathbb{F}}_p \xrightarrow{\sim} \bigoplus_{\tau_j\in S}(k\bigotimes_{k,\tau_j}\overline{\mathbb{F}}_p)(\omega^{s_i}_{\tau_j,f})$$

So restricting to the i-th component we get a surjection

$$\mathrm{H}^1(G_K,\overline{\mathbb{F}}_p(\psi)) \twoheadrightarrow \mathrm{Hom}_{\overline{\mathbb{F}}_p[G]}((k\bigotimes_{k,\tau_i}\overline{\mathbb{F}}_p)(\omega^{s_i}_{\tau_i,f}),\overline{\mathbb{F}}_p(\psi)) \ .$$

Since $\psi=\omega^c_{\tau_0,f}$, we get that

$$\mathrm{Hom}_{\overline{\mathbb{F}}_p[G]}((k\bigotimes_{k,\tau_i}\overline{\mathbb{F}}_p)(\omega^{s_i}_{\tau_i,f}),\overline{\mathbb{F}}_p(\psi)) = \mathrm{Hom}_{\overline{\mathbb{F}}_p[G]}(\overline{\mathbb{F}}_p(\omega^{s_i}_{\tau_i,f}),\overline{\mathbb{F}}_p(\omega^c_{\tau_0,f})).$$

In particular we have that the space

$$\mathrm{Hom}_{\overline{\mathbb{F}}_p[G]}((k\bigotimes_{k,\tau_i}\overline{\mathbb{F}}_p)(\omega^{s_i}_{\tau_i,f}),\overline{\mathbb{F}}_p(\psi))$$

is in fact 1-dimensional over $\overline{\mathbb{F}}_p$. So with respect to the basis of lemma 2.2.18 we get a surjection

$$\nu_{i-1}:\mathrm{H}^1(G_K,\overline{\mathbb{F}}_p(\psi)) \twoheadrightarrow \overline{\mathbb{F}}_p \ ,$$

given by

$$c \longmapsto c(E_p(\pi_L^{s_i})) \ .$$

which is well-defined up to a scalar in $\overline{\mathbb{F}}_p^{\times}$. Then the conjecture in the strongly generic case is the following:

Conjecture 2.2.19. *Let $\alpha=(V,J)\in W'(\chi_1,\chi_2)$. Then*

$$L_\alpha=\bigcap_{i\notin J} ker\ \nu_i$$

with equality in the space $H^1(G_K,\overline{\mathbb{F}}_p(\psi))$.

We would like to remark that conjecture 2.2.19 is a special case of the conjecture stated in [8] (which includes the non-generic case). Their notation has some differences from ours. They write χ for our character ψ, M for its splitting field and L for its maximal unramified subextension. Moreover they write π for a uniformizer of M, whereas we reserve the notation π for the uniformizer of $X_{\mathbb{Q}_p}$ as defined in 1.8.

Chapter 3

Proof of the Dembélé-Diamond-Roberts conjecture in the strongly generic case

As in the previous chapters $K = \mathbb{Q}_q$, where $q = p^f$ and residue field k. We fix $-p$ as a uniformizer of K and drop the uniformizer subscript from the fundamental character defined on G_K. Recall we are in the strongly generic case (in the sense of definition 2.2.3) and let us write

$$\rho_\psi : G_K \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

$$g \longmapsto \begin{pmatrix} \psi(g) & c_\rho(g) \\ 0 & 1 \end{pmatrix}.$$

where $\psi = \chi_1\chi_2^{-1} = \omega_{\tau_0,f}^d : G_K \longrightarrow \overline{\mathbb{F}}_p$, $d = \sum_{i=0}^{f-1} d_i p^i$ and put $c_{i-1} := p - 1 - d_i$. Recall that in the strongly generic case $e = p^f - 1$ and the splitting field L of ψ is given by $L = K(\sqrt[e]{-p})$, which contains all the p-th roots of unity. Notice that ψ is in fact $\mathbb{F}_q$ valued and $c_\rho \in \mathrm{H}^1(G_K, \bar{\mathbb{F}}_p(\psi))$, but the subspaces we want to show are equal in conjecture 2.2.19 are defined over $\mathbb{F}_q$, i.e. of the form $V \underset{\mathbb{F}_q}{\otimes} \bar{\mathbb{F}}_p$ for $V \subset \mathrm{H}^1(G_K, \mathbb{F}_q(\psi))$.

So we can assume c_ρ is $\mathbb{F}_q$ valued.

Recall from section 2.2, that we have an injective map

$$\phi : W(\rho) \setminus W_{\text{excep.}}(\rho) \longrightarrow \{J : J \subset S\} \setminus J_{\text{excep.}}(\rho)$$

$$V \longmapsto J_{\max}(V).$$

Since we assume strong genericity, we have that $W_{\text{excep.}}(\rho)$ and $J_{\text{excep.}}(\rho)$ are empty. Lemma 2.2.2 allows us to define an injective map

$$\alpha : \{J : J \subset S\} \longrightarrow W'(\chi_1, \chi_2)$$

$$J \longmapsto (V(J), J),$$

where $V(J) = V_{\vec{m},\vec{n}}$. These two maps satisfy the relations $\pi_1 \circ \alpha(J_{\max}(V)) = V$ and if $\pi_1 \circ \alpha(J) \in W(\rho)$, then $J_{\max}(\pi_1 \circ \alpha(J)) = J$. We have that α surjects onto $W'(\chi_1, \chi_2)$. So we can relabel $L_\alpha = L_{\alpha(J)}$ by L_J, for α an element of $W'(\chi_1, \chi_2)$.

Recall in proposition 1.9.2 we had a classication of rank one (ϕ, Γ_K)-modules over $\mathbb{E}_{K,F}$, for F a finite extension of $\mathbb{Q}_p$. Using lemma 3.8 of [6], the authors of the paper [7] obtain the following result (corollary 3.3 of [7]).

Lemma 3.0.20. *Let $\xi : G_K \longrightarrow k_F^\times$ be the character defined by the action on $\boldsymbol{V}(M_{C,\vec{c}})$. Then we have* $\xi|_{I_K} = \prod_{0 \le i \le f-1} \omega_{\tau_i,f}^{-c_{i-1}} = \omega_{\tau_0,f}^{-\sum_{i=0}^{f-1} c_{i-1}p^i} = \omega_{\tau_0,f}^{p^f-1-\sum_{i=0}^{f-1} c_{i-1}p^i}$.

Notice that in our setup $\mathbf{V}(M_{C,\vec{c}})$ defines the character $\psi = \omega_{\tau_0,f}^d$, with $F = \mathbb{F}_q$. Recall in section 2.2 we have defined the integers $s_j = \sum_{k=0}^{f-1} c_{j+k+1}p^k$. Over the strongly generic range $s_j \le (p-2)\frac{p^f-1}{p-1} = (p-2)t$ and $s_j > \frac{p^f-1}{p-1} = t$. Hence $p^f - 1 - (p-2)\frac{p^f-1}{p-1} = t \le p^f - 1 - s_j < p^f - 1 - t$ and we can work over the range $\pi_L^t/\pi_L^{p^f-1-t}$. Let us define

$$m_j := \sum_{k=0}^{f-1} d_{j+k+1}p^k,$$

which satisfies $m_j = p^f - 1 - s_{j-1}$. Following lemma 2.2.18 we can work with

$$\{E_p(a\pi_L^{m_j}) \bmod U_L^{p^f-1-t}(L^\times)^p \cap U_L^t : 0 \leq j \leq f-1\},$$

which are also linearly independent.

In the paper [7], the authors parametrize a subspace $V_J \subset \mathrm{Ext}^1(M_0, M_{C,\vec{c}})$, where each element corresponds to some rank two (ϕ, Γ_K)-module in $\mathrm{Mod}_{\mathbb{E}_{K,K}}^{\phi,\Gamma,\acute{e}t}$, which contains as a submodule the rank one (ϕ,Γ_K)-module $\mathbf{D}(\mathbb{F}_q(\psi))$ and as a quotient the trivial (ϕ,Γ_K)-module. They define certain (ϕ,Γ_K)-modules B_i which serve as a basis of V_J. In particular, they have the following result (proposition 5.4 of [7]).

Proposition 3.0.21. *If $0 < c_i < p-1$ for all $i \in S$, then $V_{\{i\}} = \mathbb{F}_q B_{i+1}$ for all $i \in S$ and $V_J = \bigoplus_{i \in J} V_{\{i\}}$ for $J \subset S$.*

Notice that the equivalence of the categories $\mathrm{Mod}_{\mathbb{E}_{K,K}}^{\phi,\Gamma,\acute{e}t}$ and $\mathrm{Rep}_{\mathbb{F}_q} G_K$ implies the isomorphism $\mathrm{Ext}^1(M_0, M_{C,\vec{c}}) \cong \mathrm{H}^1(G_K, \mathbb{F}_q(\psi))$. The importance of these subspaces V_J is the following result (remark 7.7 and theorem 7.8 (1) of [7]).

Theorem 3.0.22. *Suppose $\vec{c}$ satisfies $c_i \in \{1, ..., p-2\}$ for all $i \in S$. Suppose also that for $J \subset S$, $J \neq S$ (resp. $J \neq \emptyset$) if $\vec{c} = \overrightarrow{p-2}$ (resp. $\vec{c} = \vec{1}$). Then $L_{J'} = V_J$, where $J = \{i : i-1 \in J'\}$.*

Definition 3.0.23. For $i \in S \setminus S'$, we define the following elements of $\mathrm{H}^1_{\mathrm{ty}}/\mathrm{H}^1_{\mathrm{gt}}$:

$$\delta_i(\mathrm{pr} \circ E_p(\pi_L^{m_j})) := \begin{cases} 1, & \text{if } j = i \\ 0, & \text{otherwise} \end{cases}$$

where $\mathrm{pr} : U_L^t/U_L^{p^f-1-t} \longrightarrow U_L^t/U_L^{p^f-1-t}(L^\times)^p \cap U_L^t$.

Then we have that $\{\nu_i\}_{i\in S\setminus S'}$ is a basis for the dual $(\mathrm{H}^1_{\mathrm{ty}}/\mathrm{H}^1_{\mathrm{gt}})^*$ and $\ker\,\nu_j = \bigoplus_{k\neq j+2}\mathbb{F}_q(\delta_k)$. Thus it follows that

$$\bigcap_{j\in S\setminus J_{\max}(V)}\ \bigoplus_{k\neq j+2}\mathbb{F}_q(\delta_k) = \bigoplus_{j\in J_{\max}(V)}\mathbb{F}_q(\delta_{j+2})$$

and

$$\bigoplus_{i\in J_{\max}(V)}\ \bigcap_{j\in S\setminus\{i\}}\ \bigoplus_{l\neq j+2}\mathbb{F}_q(\delta_l) = \bigoplus_{i\in J_{\max}(V)}\mathbb{F}_q(\delta_{i+2}).$$

So we have the following lemma.

Lemma 3.0.24.

$$\bigcap_{j\in S\setminus J_{max}(V)} \mathit{ker}\ \nu_j = \bigoplus_{i\in J_{max}(V)}\ \bigcap_{j\in S\setminus\{i\}} \mathit{ker}\ \nu_j$$

We can then restate the conjecture as

$$L_{J_{\max}(V)} = \bigoplus_{i\in J_{\max}(V)} L_{\{i\}} = \bigoplus_{i\in J_{\max}(V)}\ \bigcap_{j\in S\setminus\{i\}} \ker\ \nu_{j+1}.$$

In particular, to prove conjecture 2.2.19 it suffices to prove

$$L_{\{i\}} = \bigcap_{j\in S\setminus\{i\}} \ker\ \nu_{j+1}.$$

Notice that $\bigcap_{j\in S\setminus\{i\}} \ker\ \nu_{j+1} = \bigcap_{j\in S\setminus\{i\}}\ \bigoplus_{k\neq j+3}\mathbb{F}_q(\delta_k) = \mathbb{F}_q(\delta_{i+3})$ which is 1-dimensional over $\mathbb{F}_q$ and so is $L_{\{i\}}$. Hence to prove the conjecture it suffices to prove the inclusion

$$L_{\{i\}} \subset \bigcap_{j\in S\setminus\{i\}} \ker\ \nu_{j+1}.$$

3.1 Computing the representation from the (ϕ,Γ)-module

Recall that we had $S = \{\tau_0, \tau_1 = \tau_0\circ\phi, ..., \tau_{f-1} = \tau_0\circ\phi^{f-1}\}$, where now τ_0 is some fixed embedding $k \hookrightarrow \overline{\mathbb{F}}_p$. For B_i a basis element of $\mathrm{Ext}^1(M_0, M_{C,\vec{c}})$ (as defined in [7]) we have that $B_i = \bigoplus_{\tau_j \in S} e_{\tau_j} B_i$. We assume $C = 1$ and we will see in corollary 3.3.15 that this implies that $\mathbf{V}(M_{1,\vec{c}})$ has trivial unramified twist.

Since $\psi = \omega^c_{\tau_0,f}$ is valued in $\mathbb{F}_q = \tau_0(k)$ we have that B_i is defined over $\mathbb{E}_{K,K}$. Notice that $\mathbb{E}_{K,K} = \mathbb{E}_K \bigotimes_{\mathbb{F}_p} \mathbb{F}_q \cong \bigoplus_{\tau_j \in S} \mathbb{F}_q((\pi)) \cong \bigoplus_{\tau_j \in S} k((\pi)) = \bigoplus_{\tau_j \in S} \mathbb{E}_K$, since $\mathbb{F}_q \cong k$. We have that $B_i \bigotimes_{\mathbb{E}_K} \mathbb{E} = \bigoplus_{\tau_j \in S} (e_{\tau_j} B_i \bigotimes_{\mathbb{E}_K} \mathbb{E})$ over $\mathbb{F}_q \bigotimes_{\mathbb{F}_p} \mathbb{E} \cong \bigoplus_{\tau_j \in S} \mathbb{E}$.

Let us write w_1, w_2 for the basis elements of B_i such that (following [7]) the action of ϕ and $\gamma \in \Gamma$ is given by

$$P := \begin{pmatrix} \kappa_\phi & \mu_\phi \\ 0 & 1 \end{pmatrix}, Q := \begin{pmatrix} \kappa_\gamma & \mu_\gamma \\ 0 & 1 \end{pmatrix},$$

where $\kappa_\phi = (\pi^{(p-1)c_0}, \pi^{(p-1)c_1}, ..., \pi^{(p-1)c_{f-1}})$ and $\mu_\phi = (0, ..., 0, H_i(\pi), 0, ..., 0)$. Here $H_i(\pi) = \pi^{1-p} + \epsilon_{2-p}\pi^{2-p} + ... + \epsilon_{-1}\pi^{-1}$, for some $\epsilon_{2-p}, ..., \epsilon_{-1} \in \mathbb{F}_p$ satisfying certain conditions (see [7], section 4.1). In this section we would like to write down a basis $\{t_1, t_2\}$ for the representation $\mathbf{V}(B_i)$.

We first consider the vector

$$t_1 := \alpha w_1 \in \bigoplus_{\tau_j \in S} (e_{\tau_j} B_i \bigotimes_{\mathbb{E}_K} \mathbb{E}),$$

where $\alpha := (\alpha_0, ..., \alpha_{f-1}) \in \bigoplus_{\tau_j \in S} \mathbb{E}$. So we have

$$t_1 = \left(\begin{pmatrix} \alpha_0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} \alpha_1 \\ 0 \end{pmatrix}, \quad ..., \quad \begin{pmatrix} \alpha_{f-1} \\ 0 \end{pmatrix} \right).$$

If t_1 is in fact an element of $\mathbf{V}(B_i)$ then it must satisfy $\phi(t_1) = t_1$. The semilinear action of ϕ is given by

$$\phi(t_1) = \left(e_{\tau_1} \phi \begin{pmatrix} \alpha_1 \\ 0 \end{pmatrix}, \quad e_{\tau_2} \phi \begin{pmatrix} \alpha_2 \\ 0 \end{pmatrix}, \quad ..., \quad e_{\tau_{f-1}} \phi \begin{pmatrix} \alpha_{f-1} \\ 0 \end{pmatrix}, \quad e_{\tau_0} \phi \begin{pmatrix} \alpha_0 \\ 0 \end{pmatrix} \right).$$

Here $e_{\tau_j}\phi\begin{pmatrix}\alpha_j\\0\end{pmatrix}=P_{j-1}\begin{pmatrix}\alpha_j^p\\0\end{pmatrix}$ and $P_j=\begin{pmatrix}\kappa_{\phi_j} & \mu_{\phi_j}\\0 & 1\end{pmatrix}$. This gives the following equations:

$$\alpha_0=\kappa_{\phi_0}\alpha_1^p$$

$$\alpha_1=\kappa_{\phi_1}\alpha_2^p$$

$$\vdots$$

$$\alpha_{f-2}=\kappa_{\phi_{f-2}}\alpha_{f-1}^p$$

$$\alpha_{f-1}=\kappa_{\phi_{f-1}}\alpha_0^p.$$

Solving these we get

$$\alpha_j^{p^f-1}=(\kappa_{\phi_j}\kappa_{\phi_{j+1}}^p...\kappa_{\phi_{f-1}}^{p^{f-j-2}}\kappa_{\phi_0}^{p^{f-j-1}}\kappa_{\phi_1}^{p^{f-j}}...\kappa_{\phi_{j-1}}^{p^{f-1}})^{-1},$$

and expanding

$$\alpha_j^{p^f-1}=\pi^{-(p-1)(c_j+pc_{j+1}+...+p^{f-j-1}c_{f-1}+p^{f-j}c_0+p^{f-j+1}c_1+...+p^{f-1}c_{j-1})}.$$

Recall from section 2.2 that we had that $s_j=\sum_{k=0}^{f-1}c_{k+j+1}p^k$. Thus we get $\alpha_j^{p^f-1}=\pi^{-(p-1)s_{j-1}}$ and so for $0\leq j\leq f-1$,

$$\alpha_j=\pi^{-\frac{(p-1)s_{j-1}}{p^f-1}}=\pi^{\frac{-s_{j-1}}{t}}.$$

We are now after the second linearly independent vector in $\mathbf{V}(B_i)$. Consider the vector

$$t_2:=\beta w_1+w_2\in\bigoplus_{\tau_j\in S}(e_{\tau_j}B_i\bigotimes_{\mathbb{E}_K}\mathbb{E}),$$

where $\beta:=(\beta_0,...,\beta_{f-1})\in\bigoplus_{\tau_j\in S}\mathbb{E}$. So we can write

$$t_2=\left(\begin{pmatrix}\beta_0\\1\end{pmatrix},\quad ...,\quad\begin{pmatrix}\beta_{f-1}\\1\end{pmatrix}\quad\right).$$

It is clear that t_2 is linearly independent from t_1 and t_2 needs to satisfy $\phi(t_2) = t_2$, that is

$$P_j \begin{pmatrix} \beta_{j+1}^p \\ 1 \end{pmatrix} = \begin{pmatrix} \kappa_{\phi_j}\beta_{j+1}^p + \mu_{\phi_j} \\ 1 \end{pmatrix} = \begin{pmatrix} \beta_j \\ 1 \end{pmatrix}.$$

So we get the equations

$$\beta_0 = \kappa_{\phi_0}\beta_1^p$$

$$\beta_1 = \kappa_{\phi_1}\beta_2^p$$

$$\vdots$$

$$\beta_i = \kappa_{\phi_i}\beta_{i+1}^p + H_i(\pi)$$

$$\vdots$$

$$\beta_{f-2} = \kappa_{\phi_{f-2}}\beta_{f-1}^p$$

$$\beta_{f-1} = \kappa_{\phi_{f-1}}\beta_0^p.$$

Solving these equations we find that β_j satisfies the following:

- $j < i$:

  $$\kappa_{\phi_j}\kappa_{\phi_{j+1}}^p ... \kappa_{\phi_{f-1}}^{p^{f-j-1}}\kappa_{\phi_0}^{p^{f-j}} ... \kappa_{\phi_{j-1}}^{p^{f-1}} Z^{p^f} - Z + \kappa_{\phi_j} ... \kappa_{\phi_{i-1}}^{p^{i-j-1}} H_i^{p^{i-j}}(\pi) = 0.$$

  Let

  $$a := (p-1)(p^{f-j}c_0 + p^{f-j+1}c_1 + ... + p^{f-1}c_{j-1} + c_j + pc_{j+1} + ... + p^{f-j-1}c_{f-1}),$$

  $$b := (p-1)(c_j + pc_{j+1} + ... + p^{i-j-1}c_{i-1}).$$

  But $a = (p-1)s_{j-1}$ and so we can rewrite the polynomial as

  $$Z^{p^f} - \pi^{-(p-1)s_{j-1}} Z + \pi^{-(p-1)s_{j-1}+b} H_i^{p^{i-j}}(\pi) = 0.$$

We can also write

$$\beta_j = \kappa_{\phi_j}\kappa_{\phi_{j+1}}^p ... \kappa_{\phi_{i-1}}^{p^{i-1-j}} \beta_i^{p^{i-j}}.$$

- $j = i$:

$$\kappa_{\phi_i}\kappa_{\phi_{i+1}}^p ... \kappa_{\phi_{f-1}}^{p^{f-i}} \kappa_{\phi_0}^{p^{f-i+1}} ... \kappa_{\phi_{i-1}}^{p^{f-1}} Z^{p^f} - Z + H_i(\pi) = 0,$$

or

$$Z^{p^f} - \pi^{-(p-1)s_{i-1}} Z + \pi^{-(p-1)s_{i-1}} H_i(\pi) = 0.$$

- $j > i$:

$$\kappa_{\phi_j}\kappa_{\phi_{j+1}}^p ... \kappa_{\phi_{f-1}}^{p^{f-j}} \kappa_{\phi_0}^{p^{f-j+1}} ... \kappa_{\phi_{j-1}}^{p^{f-1}} Z^{p^f} - Z + \kappa_{\phi_j} ... \kappa_{\phi_{f-1}}^{p^{f-j}} \kappa_{\phi_0}^{p^{f-j+1}} ... \kappa_{\phi_{i-1}}^{p^{f-j+i-1}} H_i^{p^{f+i-j}}(\pi) = 0.$$

Let

$$d := (p-1)(c_j + pc_{j+1} + ... + p^{f-j}c_{f-1} + p^{f-j+1}c_0 + ... + p^{f-j+i-1}c_{i-1})).$$

Then we can rewrite the polynomial as

$$Z^{p^f} - \pi^{-(p-1)s_{j-1}} Z + \pi^{-(p-1)s_{j-1}+d} H_i^{p^{f+i-j}}(\pi) = 0.$$

We can also write

$$\beta_j = \kappa_{\phi_j}\kappa_{\phi_{j+1}}^p ... \kappa_{\phi_{f-1}}^{p^{f-1-j}} \kappa_{\phi_0}^{p^{f-j}} ... \kappa_{\phi_{i-1}}^{p^{f+i-1-j}} \beta_i^{p^{f+i-j}}.$$

By functoriality we have that $\mathbb{F}_q t_1$ is a subrepresentation of $\mathbf{V}(B_i)$. Summarizing, we have the following result:

Proposition 3.1.1. *The vectors $t_1 = \alpha w_1$, $t_2 = \beta w_1 + w_2$ form a basis of the representation $\boldsymbol{V}(B_i)$ over $\mathbb{F}_q$. In particular $\mathbb{F}_q t_1$ is a subrepresentation of $\boldsymbol{V}(B_i)$ and the image of t_2 in $\boldsymbol{V}(B_i)/\mathbb{F}_q t_1$ is a basis.*

We conclude this section by computing the action of $G_{\mathbb{E}_K} \cong H_K$ on $\mathbb{F}_q t_1$. Notice that $\alpha_j \in \mathbb{E}_K(\pi^{1/t})$ for all j and $\mathbb{E}_K(\pi^{1/t})/\mathbb{E}_K$ is a Kummer extension. Let ω' be the k-valued fundamental character associated by Kummer theory to $\pi^{1/t}$ and consider its $\mathbb{F}_q$-valued embedding $\tau_0 \circ \omega'$.

Lemma 3.1.2. *For $g \in Gal(\mathbb{E}_K(\pi^{1/t})/\mathbb{E}_K)$,*

$$g \cdot t_1 = (\tau_0 \circ \omega')^{-c} t_1.$$

Proof. We have that

$$\begin{aligned} g \cdot t_1 &= (g \cdot \alpha) w_1 \\ &= (g \cdot \alpha_0, ..., g \cdot \alpha_{f-1}) w_1 \\ &= (g \cdot \pi^{-s_{f-1}/t}, g \cdot \pi^{-s_0/t}, ..., g \cdot \pi^{-s_{f-2}/t}) w_1 \\ &= (\omega'^{-c}, \omega'^{-pc}, ..., \omega'^{-p^{f-1}c}) t_1 \\ &= (\tau_0 \circ \omega')^{-c} t_1. \end{aligned}$$

□

3.2 Distinguished subspaces of $\mathbf{H}^1(G_{X_L}, \overline{\mathbb{F}}_p(\psi))$

In this section we consider the restriction of ρ_ψ, that we now assume has underlying vector space $\mathbf{V}(B_i)$, to G_L given by

$$\rho_\psi|_{G_L}(g) = \begin{pmatrix} 1 & c_\rho(g) \\ 0 & 1 \end{pmatrix}.$$

Recall from section 1.9, $\mathbf{V}(B_i)$ has an action of G_{X_K}. In section 3.1 we wrote a $\mathbb{F}_q$ basis $\{t_1, t_2\}$ of $\mathbf{V}(B_i)$. The action of G_{X_K} is then given by $\begin{pmatrix} \psi' & c'_\rho \\ 0 & 1 \end{pmatrix}$, where

$c'_\rho \in \mathrm{H}^1(G_{X_K}, \mathbb{F}_q(\psi'))$. Here $\psi' : G_{X_K} \longrightarrow \mathbb{F}_q^\times$ can be pulled back to G_{K_∞} by the field of norms isomorphism $G_{K_\infty} \cong G_{X_K}$ and by the equivalence of categories (theorem 1.8.2) we have that ψ' pulls back to $\psi|_{G_{K_\infty}}$. As a result the splitting field of ψ' is X_L. Restricting the action of G_{X_K} on $\mathbf{V}(B_i)$ to G_{X_L} we get a homomorphism $c'_\rho \in \mathrm{Hom}_{\mathbb{F}_p[\mathrm{Gal}(X_L/X_K)]}(G_{X_L}, \mathbb{F}_q(\psi')) \cong \mathrm{Hom}_{\mathbb{F}_p[G]}(G_{L_\infty}, \mathbb{F}_q(\psi))$, after applying the field of norms isomorphism. Moreover, as for ψ', we have that c'_ρ also pulls back to $c_\rho|_{G_{K_\infty}}$.

The kernel of c_ρ is an open subgroup of G_L and so it factors through a finite abelian quotient $\mathrm{Gal}(M/L)$ of G_L.

Definition 3.2.1. We write M for the extension of L that is the splitting field of c_ρ and X_M for the extension of X_L that corresponds to the splitting field of c'_ρ. In particular, X_M is the field of norms of M_∞.

We remark that in [8], the authors write N for the field M. Recall that c'_ρ defines a homomorphism $G_{X_L} \longrightarrow \mathbb{F}_q$. Let us write $c'_{\rho,j} : G_{X_L} \longrightarrow k$ (respectively $c_{\rho,j} : G_{X_L} \longrightarrow k$), where we compose c'_ρ (respectively c_ρ) with the inverse of the isomorphism $\tau_j : k \longrightarrow \mathbb{F}_q$.

Proposition 3.2.2. *Consider the elements α, β defined in section 3.1 and let $z := -\frac{\beta}{\alpha} \in \mathbb{E}_{M,K}$. Then we have that for $g \in Gal(X_M/X_L)$*

$$c'_\rho(g) = g \cdot (-z) - (-z).$$

Moreover if $\tau_j \in S$ we get that

$$c'_{\rho,j}(g) = g \cdot (-z_j) - (-z_j).$$

Proof. Recall that we had that $t_1 = \alpha w_1$ and $t_2 = \beta w_1 + w_2$ as basis vectors of $(B_i \bigotimes_{\mathbb{E}_K} \mathbb{E})^{\phi=1} = (\bigoplus_{\tau_j \in S} (e_{\tau_j} B_i \bigotimes_{\mathbb{E}_K} \mathbb{E}))^{\phi=1}$. From proposition 3.1.1 an element $g \in H_L \cong$

G_{X_L} acts trivially on the vector t_1 and $g \cdot t_2 = c'_\rho(g)t_1 + t_2$ we have that

$$c'_{\rho,0}(g)\alpha_0 = (g-1)\beta_0$$

$$\vdots$$

$$c'_{\rho,i}(g)\alpha_i = (g-1)\beta_i$$

$$\vdots$$

$$c'_{\rho,f-1}(g)\alpha_{f-1} = (g-1)\beta_{f-1}.$$

Thus we may write

$$c'_{\rho,j}(g) = g \cdot \frac{\beta_j}{\alpha_j} - \frac{\beta_j}{\alpha_j}.$$

□

Proposition 3.2.3. *We have that*

$$\phi(z) - z = \frac{\mu_\phi}{\alpha} = (0, ..., 0, \frac{H_i(\pi)}{\alpha_i}, 0, ..., 0).$$

Moreover writing $z = (z_0, ..., z_{f-1})$*, we have*

$$z_j^{p^f} - z_j - \left(\frac{H_i(\pi)}{\alpha_i}\right)^{p^{i-j}} = 0$$

for $0 \leq j \leq f-1$*.*

Proof. Recall that we defined $z = -\frac{\beta}{\alpha}$. So we have that

$$(\phi(z) - z)_j = -\frac{\beta_{j+1}^p}{\alpha_{j+1}^p} + \frac{\beta_j}{\alpha_j} = \frac{-\kappa_{\phi_j}\beta_{j+1}^p + \beta_j}{\alpha_j},$$

where we have used the relation $\kappa_{\phi_j}\alpha_{j+1}^p = \alpha_j$ from section 3.1. But we also have from section 3.1 that $-\kappa_{\phi_j}\beta_{j+1}^p + \beta_j = 0$ if $j \neq i$ and equal to $H_i(\pi)$ if $j = i$. Hence we get that

$$(\phi(z) - z)_j = z_{j+1}^p - z_j = \begin{cases} 0, & \text{if } j \neq i \\ \\ \frac{H_i(\pi)}{\alpha_i}, & \text{if } j = i. \end{cases}$$

Hence we have the relations

$$z_0 = z_1^p$$

$$\vdots$$

$$z_{i-1} = z_i^p$$

$$z_i = z_{i+1}^p - \frac{H_i(\pi)}{\alpha_i}$$

$$z_{i+1} = z_{i+2}^p$$

$$\vdots$$

$$z_{f-2} = z_{f-1}^p$$

$$z_{f-1} = z_0^p.$$

Solving for z_j gives the result. $\square$

Let us write V_{c_ρ} for the underlying G_L vector space of the representation $\rho_\psi|_{G_L}$. Then we want to write down a basis for the (ϕ, Γ_L)-module corresponding to this representation. Recall that the functor is given by $\mathbf{D}_{G_{X_L}}(V_{c_\rho}) = (V_{c_\rho} \bigotimes_{\mathbb{F}_p} \mathbb{E})^{H_L}$, where $H_L \cong G_{X_L}$ under the field of norms isomorphism and $\mathbf{D}_{G_{X_L}}(V_{c_\rho})$ is a (ϕ, Γ_L)-module over $\mathbb{E}_{L,K}$.

Proposition 3.2.4. *Let* $f_1 := t_1 \bigotimes 1$ *and* $f_2 := t_1 \bigotimes z + t_2 \bigotimes 1$ *be elements of* $V_{c_\rho} \bigotimes_{\mathbb{F}_p} \mathbb{E}$.

Then we have that f_1 and f_2 are basis vectors of $\boldsymbol{D}_{G_{X_L}}(V_{c_\rho})$ over $\mathbb{E}_{L,K}$. Moreover, the ϕ-action on $\boldsymbol{D}_{G_{X_L}}(V_{c_\rho})$ under this basis is given by

$$\begin{pmatrix} 1 & \phi(z)-z \\ 0 & 1 \end{pmatrix}$$

where $(\phi(z)-z)_j = z_{j+1}^p - z_j$.

Proof. Given $g \in H_L \cong G_{X_L}$, we have that

$$g \cdot f_1 = f_1$$

and

$$g \cdot f_2 = t_1 \bigotimes g \cdot z + (c'_\rho(g)t_1 + t_2) \bigotimes 1.$$

Since $c'_\rho(g) = g \cdot (-z) + z$, we have that the previous expression is equal to

$$t_1 \bigotimes g \cdot z + (g \cdot (-z) + z)t_1 \bigotimes 1 + t_2 \bigotimes 1 = t_1 \bigotimes z + t_2 \bigotimes 1 = f_2.$$

It is also clear that f_1 and f_2 are linearly independent over $\mathbb{E}_{L,K}$ and so we have that f_1 and f_2 are basis vectors of $\mathbf{D}_{G_{X_L}}(V_{c_\rho})$ over $\mathbb{E}_{L,K}$.

For the ϕ action we notice that f_1 is ϕ invariant and

$$\begin{aligned} \phi \cdot f_2 &= t_1 \bigotimes \phi \cdot z + t_2 \bigotimes 1 \\ &= t_1 \bigotimes (\phi \cdot z - z + z) + t_2 \bigotimes 1 \\ &= t_1 \bigotimes (\phi \cdot z - z) + t_1 \bigotimes z + t_2 \bigotimes 1 \\ &= t_1 \bigotimes (\phi \cdot z - z) + f_2. \end{aligned}$$

Since $\phi \cdot f_2 \in \mathbf{D}_{G_{X_L}}(V_{c_\rho})$, we have that $\phi \cdot z - z \in \mathbb{E}_{L,K}$. So

$$t_1 \bigotimes (\phi \cdot z - z) = (1 \bigotimes (\phi \cdot z - z))f_1.$$

Hence

$$\begin{aligned} e_{\tau_j}(1\bigotimes(\phi\cdot z - z)) &= e_{\tau_j}(1\bigotimes \phi\cdot z) - e_{\tau_j}(1\bigotimes z) \\ &= \phi\cdot e_{\tau_{j+1}}(1\bigotimes z) - e_{\tau_j}(1\bigotimes z) \\ &= z_{j+1}^p - z_j. \end{aligned}$$

□

The next lemma will allow us to extend coefficients on our (ϕ,Γ)-module B_i. For this we will need the result of Galois descent on vector spaces:

Theorem 3.2.5. *Let L/K be a finite Galois extension with Galois group G and V a L -vector space equipped with a semi-linear G-action, i.e. a G-action satisfying $g(lv) = g(l)g(v)$ for all $g\in G, v\in V$ and $l\in L$. Then the natural map*

$$V^G\bigotimes_K L \longrightarrow V$$

$$v\bigotimes l \longmapsto lv$$

is an isomorphism.

Proof. This is lemma 2.3.8 in [16]. □

Lemma 3.2.6.

$$\boldsymbol{D}_{G_{X_L}}(Res^{G_{X_K}}_{G_{X_L}}V_{c_\rho}) = (Res^{G_{X_K}}_{G_{X_L}}V_{c_\rho}\bigotimes_{\mathbb{F}_p}\mathbb{E})^{G_{X_L}} \cong \boldsymbol{D}_{G_{X_K}}(V_{c_\rho})\bigotimes_{\mathbb{E}_K}\mathbb{E}_L,$$

as (ϕ,Γ_L)-modules. The ϕ and γ action on $\boldsymbol{D}_{G_{X_K}}(V_{c_\rho})\bigotimes_{\mathbb{E}_K}\mathbb{E}_L$ is given by $\phi_{\boldsymbol{D}_{G_{X_K}}(V_{c_\rho})}\bigotimes\phi_{\mathbb{E}_L}$ and $\gamma_{\boldsymbol{D}_{G_{X_K}}(V_{c_\rho})}\bigotimes\gamma_{\mathbb{E}_L}$ respectively.

Proof. We first check that $\mathbf{D}_{G_{X_K}}(V_{c_\rho})\bigotimes_{\mathbb{E}_K}\mathbb{E}_L$ is an étale (ϕ,Γ_L)-module, over $\mathbb{E}_{L,K}$. In particular, the only thing that needs check is étaleness. Since $\mathbf{D}_{G_{X_K}}(V_{c_\rho})$ is étale, we have that $\phi : \mathbf{D}_{G_{X_K}}(V_{c_\rho}) \longrightarrow \mathbf{D}_{G_{X_K}}(V_{c_\rho})$ spans $\mathbf{D}_{G_{X_K}}(V_{c_\rho})$ over $\mathbb{E}_{K,K}$. Suppose $\sum_i m_i \bigotimes l_i \in \mathbf{D}_{G_{X_K}}(V_{c_\rho}) \bigotimes_{\mathbb{E}_K} \mathbb{E}_L$ and $m_i = \sum_j a_{ij}\phi(m_{ij})$, $a_{ij} \in \mathbb{E}_{K,K}$, $m_{ij} \in \mathbf{D}_{G_{X_K}}(V_{c_\rho})$. Then we have that

$$\begin{aligned}\sum_i m_i \bigotimes l_i &= \sum_i l_i(m_i \bigotimes 1)\\ &= \sum_i l_i((\sum_j a_{ij}\phi(m_{ij})) \bigotimes 1)\\ &= \sum_i l_i \sum_j a_{ij}\phi(m_{ij} \bigotimes 1)\\ &= \sum_{i,j} l_i a_{ij}\phi(m_{ij} \bigotimes 1).\end{aligned}$$

Hence $\phi : \mathbf{D}_{G_{X_K}}(V_{c_\rho}) \bigotimes_{\mathbb{E}_K} \mathbb{E}_L \longrightarrow \mathbf{D}_{G_{X_K}}(V_{c_\rho}) \bigotimes_{\mathbb{E}_K} \mathbb{E}_L$ spans $\mathbf{D}_{G_{X_K}}(V_{c_\rho}) \bigotimes_{\mathbb{E}_K} \mathbb{E}_L$ over $\mathbb{E}_{L,K}$.

Let $H := \mathrm{Gal}(X_L/X_K)$. Notice that $\mathbf{D}_{G_{X_K}}(V_{c_\rho}) = (V_{c_\rho} \bigotimes_{\mathbb{F}_p} \mathbb{E})^{G_{X_K}} = ((V_{c_\rho} \bigotimes_{\mathbb{F}_p} \mathbb{E})^{G_{X_L}})^H$ and the natural map $((V_{c_\rho} \bigotimes_{\mathbb{F}_p} \mathbb{E})^{G_{X_L}})^H \bigotimes_{\mathbb{E}_K} \mathbb{E}_L \longrightarrow (V_{c_\rho} \bigotimes_{\mathbb{F}_p} \mathbb{E})^{G_{X_L}}$ given by $(v \bigotimes z) \bigotimes l \mapsto l(v \bigotimes z)$ is an isomorphism by Galois descent 3.2.5. Moreover, it is clear that this map is ϕ and γ equivariant. Hence we get that $\mathbf{D}_{G_{X_L}}(\mathrm{Res}^{G_{X_K}}_{G_{X_L}} V_{c_\rho})$ and $\mathbf{D}_{G_{X_K}}(V_{c_\rho}) \bigotimes_{\mathbb{E}_K} \mathbb{E}_L$ are isomorphic (ϕ, Γ_L)-modules. $\square$

Corollary 3.2.7.

$$\boldsymbol{D}_{G_{X_L}}(V_{c_\rho}) \cong B_i \bigotimes_{\mathbb{E}_K} \mathbb{E}_L.$$

Recall that we wrote w_1, w_2 for the basis of B_i for which $\phi \cdot w_1 = k_\phi w_1$ and $\phi \cdot w_2 = \mu_\phi w_1 + w_2$. In section 3.1 we have shown that $\mathbb{F}_q t_1$ is a subrepresentation of $\mathbf{V}(B_i)$. Since L is defined to be the splitting field of this subrepresentation, we have by the theory of field of norms that $t_1 = \alpha w_1 \in (B_i \bigotimes_{\mathbb{E}_K} \mathbb{E}_L)^{\phi=1}$. Define the basis vectors of $B_i \bigotimes_{\mathbb{E}_K} \mathbb{E}_L$ by $\tilde{w}_1 := t_1$ and $\tilde{w}_2 := w_2$. Then we have that $\phi \cdot \tilde{w}_1 = \tilde{w}_1$ and $\phi \cdot \tilde{w}_2 = \frac{\mu_\phi}{\alpha}\tilde{w}_1 + \tilde{w}_2$. Hence we have the following result:

Lemma 3.2.8. *The action of ϕ on $B_i \bigotimes\limits_{\mathbb{E}_K} \mathbb{E}_L$ with respect to the basis $\{\tilde{w}_1, \tilde{w}_2\}$ is given by*

$$\begin{pmatrix} 1 & \frac{\mu_\phi}{\alpha} \\ 0 & 1 \end{pmatrix}.$$

3.3 The tamely and wildly ramified splitting fields

In this section we study the splitting fields L, M of ψ, c_ρ and the field of norms X_L, X_M of L_∞, M_∞.

Lemma 3.3.1. *M/L is a Kummer extension and $M = L(\sqrt[p]{a_1}, ..., \sqrt[p]{a_m})$, for some elements $a_1, ..., a_m \in L^\times$. Moreover we have that $M \cap (\mathbb{Q}_p)_\infty = \mathbb{Q}_p(\zeta_p)$.*

Proof. Recall that M/L is the splitting field of $c_\rho \in \mathrm{Hom}_{\mathbb{F}_p[G]}(G_L, \mathbb{F}_q(\psi))$. Thus $[M : L] = p^m$ and $\mathrm{Gal}(M/L)$ has exponent p. Moreover $L = K(\sqrt[e]{-p})$ and $K(\sqrt[p-1]{-p}) = K(\zeta_p) \subset L$. Thus M/L is a Kummer extension of exponent p and using 1.3.4, we get that $M = L(\sqrt[p]{a_1}, ..., \sqrt[p]{a_m})$, for some elements $a_1, ..., a_m \in L^\times$.

Suppose M contains a p^n-th root of unity for some $n > 1$. We can consider the abelian quotient $\mathrm{Gal}(K(\zeta_{p^2})/K)$ of $\mathrm{Gal}(M/K)$. $\mathrm{Gal}(K(\zeta_{p^2})/K)$ has itself a quotient of order p and hence $\mathrm{Gal}(M/K)$ has an abelian quotient of order p. On the other hand $\mathrm{Gal}(M/K)$ is isomorphic via ρ to $H := \{\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) : x \in \mathbb{F}_q^\times, y \in W\}$ where W is an $\mathbb{F}_q$ subspace of $\overline{\mathbb{F}}_p$. The calculation $\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \frac{1}{x} & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -y \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & y(x-1) \\ 0 & 1 \end{smallmatrix}\right)$ shows that every element of the form $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$ is a commutator. Thus the abelianization $H/[H, H]$ is isomorphic to a subgroup of $\mathbb{F}_q^\times$ and has order prime to p. But this contradicts the fact that $\mathrm{Gal}(M/K)$ has an abelian quotient of order p. Hence M does not contain a p^n-th root of unity for $n > 1$. Lastly, since $L = K(\sqrt[p^f-1]{-p})$ and $\mathbb{Q}_p(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_p)$, $\zeta_p \in L \subset M$. $\square$

Lemma 3.3.2.

$$[X_L : X_K] = \frac{e}{p-1} = t.$$

Proof. The theory of field of norms gives us an isomorphism $\mathrm{Gal}(X_L/X_K) \cong \mathrm{Gal}(L_\infty/K_\infty)$, which implies that $[X_L : X_K] = [L_\infty : K_\infty]$. Recall that we assume $\zeta_p \in L$ and from lemma 3.3.1, we have that $L \cap (\mathbb{Q}_p)_\infty = \mathbb{Q}_p(\zeta_p)$. Thus $\mathrm{Gal}(L_\infty/K_\infty) \cong \mathrm{Gal}(L/K(\zeta_p))$ and so $[L_\infty : K_\infty] = [L : K(\zeta_p)] = \frac{e}{p-1} = t$, by lemma 2.2.16. □

Lemma 3.3.3. *The extension X_M/X_L is a totally, wildly ramified extension, of exponent p.*

Proof. From lemma 3.3.1 we deduce that $M \cap L_\infty = L$ and so $\mathrm{Gal}(X_M/X_L) = \mathrm{Gal}(M_\infty/L_\infty) = \mathrm{Gal}(M/L)$. Since M/L is a totally, wildly ramified extension, of exponent p, so is X_M/X_L. □

Recall that in proposition 3.2.3 we have that $z_j^{p^f} - z_j - \left(\frac{H_i(\pi)}{\alpha_i}\right)^{p^{i-j}} = 0$. In particular, for $j = i$ we have the following.

Lemma 3.3.4. *The polynomial $X^q - X - \frac{H_i(\pi)}{\alpha_i}$ is irreducible over $\mathbb{E}_L$.*

Proof. We have that

$$v_{\mathbb{E}_L}(\frac{H_i(\pi)}{\alpha_i}) = \min_{1 \le k \le p-1} v_{\mathbb{E}_L}(\epsilon_{k-p}\pi^{k-p+\frac{s_{i-1}}{t}}) = t(1-p) + s_{i-1} = -p^f + 1 + s_{i-1}.$$

So the Newton polygon consists of a single line segment of slope $\frac{-p^f+1+s_{i-1}}{q}$. Moreover we have that $-p^f + 1 + s_{i-1} \equiv 1 + c_i \bmod p$. Since $c_i < p-1$, we have that $-p^f + 1 + s_{i-1} \not\equiv 0 \bmod p$. Therefore by corollary 1.5.3, we have that the polynomial $X^q - X - \frac{H_i(\pi)}{\alpha_i}$ is irreducible over $\mathbb{E}_L$. □

X_M is in fact the splitting field of $X^q - X - \frac{H_i(\pi)}{\alpha_i}$. This polynomial has as a root z_i and notice that $X_M = X_L(z_i)$ contains z_j, for all $0 \le j \le f-1$.

Corollary 3.3.5.

$$[X_M : X_L] = [M : L] = q.$$

Proof. Since X_M is the splitting field of $X^q - X - \frac{H_i(\pi)}{\alpha_i}$, we have that $[X_M : X_L] = q$. By the theory of field of norms we have that $\mathrm{Gal}(X_M/X_L) \cong \mathrm{Gal}(M_\infty/L_\infty)$ and by lemma 3.3.1, $\mathrm{Gal}(M_\infty/L_\infty) \cong \mathrm{Gal}(M/L)$. □

At this point we would like to define a uniformizer for the field X_L. For this we define the following:

Definition 3.3.6.

$$\pi_1 := \frac{1}{p-1} \sum_{\gamma \in \Delta} \chi(\gamma)^{-1} \gamma(\pi),$$

where $(\mathbb{Z}/p\mathbb{Z})^\times \cong \Delta \subset \Gamma$.

Proposition 3.3.7. *π_1 is a uniformizer of X_K. Moreover we have that for $\delta \in \Delta$, $\delta(\pi_1) = \chi(\delta)\pi_1$. In particular, $\delta((\pi_1)_k) = \chi(\delta)(\pi_1)_k$ for any $k \geq 1$.*

Proof. Notice that $\gamma(\pi) = (1+\pi)^{\chi(\gamma)} - 1$ implies that $\gamma(\pi) \equiv \chi(\gamma)\pi \bmod \pi^2$. So we have that

$$\pi_1 = \frac{1}{p-1} \sum_{\gamma \in \Delta} \chi(\gamma)^{-1} \gamma(\pi) \equiv \pi \bmod \pi^2$$

and $\frac{\pi_1}{\pi} \equiv 1 \bmod \pi$. Hence π_1 has the right valuation. We have that for $\delta \in \Delta$,

$$\begin{aligned} \delta(\pi_1) &= \frac{1}{p-1} \sum_{\gamma \in \Delta} \chi(\gamma)^{-1} \delta\gamma(\pi) \\ &= \frac{1}{p-1} \sum_{\gamma \in \Delta} \chi(\delta^{-1}\gamma')^{-1} \gamma'(\pi), \end{aligned}$$

where $\gamma' := \delta\gamma$. But this is equal to

$$\chi(\delta) \frac{1}{p-1} \sum_{\gamma' \in \Delta} \chi(\gamma')^{-1} \gamma'(\pi) = \chi(\delta)\pi_1$$

and so $\delta(\pi_1) = \chi(\delta)\pi_1$. □

Definition 3.3.8. Let $\pi_{K_1} := \sqrt[p-1]{-p}$ such that $\pi_{K_1} \equiv (\pi)_1 \bmod \pi_{K_1}^2$ be a uniformizer of $K_1 = K(\zeta_p)$.

Then we have the following.

Lemma 3.3.9. *The polynomial $X^t - (\pi_1)_1$ has a root in L. Letting $(\pi_1)_1^{1/t}$ be such a root then we have that $(\pi_1)_1^{1/t} \equiv \pi_L \bmod \pi_L^{p^f}$. In particular $(\pi_1)_1^{1/t}$ is a uniformizer of L.*

Proof. We first notice that $(\pi_1)_1 \in K_1$ and the action of Γ on K_1, factors through Δ. Hence we have that $\gamma((\pi_1)_1) = \chi(\gamma)(\pi_1)_1$ and since the fundamental character of niveau 1 is the cyclotomic character, $\gamma(\pi_{K_1}) = \chi(\gamma)\pi_{K_1}$. This implies that $\frac{(\pi_1)_1}{\pi_{K_1}}$ is fixed under the Γ_K action. Therefore $\frac{(\pi_1)_1}{\pi_{K_1}} \in \mathbb{Z}_p^\times$ and since $\frac{\pi_1}{\pi} \equiv 1 \bmod \pi$ and $\pi_{K_1} \equiv (\pi)_1 \bmod \pi_{K_1}^2$ we have that $\frac{(\pi_1)_1}{\pi_{K_1}} \equiv 1 \bmod \pi_{K_1}^{p-1}$. Next we consider the polynomial $X^t - \frac{(\pi_1)_1}{\pi_{K_1}} \equiv X^t - 1 \bmod \pi_{K_1}$. Since it's derivative evaluated at 1 is non-zero $\bmod \pi_{K_1}$, we have by Hensel's lemma that the polynomial has a root say a in K_1, that is congruent to $1 \bmod \pi_{K_1}$. But then since π_L is a t-th root of π_{K_1}, we have that $\pi_L a = (\pi_1)_1^{1/t}$ is an element of L. Let us write $a = 1 + \delta\pi_{K_1}^n$ and $\frac{(\pi_1)_1}{\pi_{K_1}} = 1 + \epsilon\pi_{K_1}^{p-1}$, for $\delta, \epsilon \in U_{K_1}$. Then we have that $1 + \epsilon\pi_{K_1}^{p-1} = a^t = (1 + \delta\pi_{K_1}^n)^t = \sum_{m=0}^t \binom{t}{m}\delta^m\pi_{K_1}^{nm}$. Hence $\epsilon\pi_{K_1}^{p-1} = (\sum_{m=1}^t \binom{t}{m}\delta^m\pi_{K_1}^{n(m-1)})\pi_{K_1}^n$ and since t is coprime to p and ϵ, δ are units we have that $n = p-1$. As a result $a \equiv 1 \bmod \pi_{K_1}^{p-1}$ and we have that $(\pi_1)_1^{1/t} \equiv \pi_L \bmod \pi_L^{p^f}$. □

The following lemma will allow us to lift $(\pi_1)_1^{1/t}$ to a uniformizer of X_L.

Lemma 3.3.10. *$Nm_{L_{n+1}/L_n} : L_{n+1}^\times/(L_{n+1}^\times)^t \longrightarrow L_n^\times/(L_n^\times)^t$ is an isomorphism.*

Proof. An application of Herbrand's quotient gives that for all $n \geq 1$, $|L_n^\times/(L_n^\times)^t| = \frac{t|\mu_t(L_n)|}{|t|_{L_n}} = t^2$. We also have that $[L_n^\times : \mathrm{Nm}_{L_{n+1}/L_n}(L_{n+1}^\times)] = [L_{n+1} : L_n] = p$. Since

p is coprime to t, $L_n^\times/(L_n^\times)^t$ has no subgroups of order p. Thus the projection of $L_n^\times/\mathrm{Nm}_{L_{n+1}/L_n}(L_{n+1}^\times)$ in $L_n^\times/(L_n^\times)^t$ is trivial and so $\mathrm{Nm}_{L_{n+1}/L_n}(L_{n+1}^\times/(L_{n+1}^\times)^t) = L_n^\times/(L_n^\times)^t$. Since $|L_n^\times/(L_n^\times)^t| = t^2$ for all $n \geq 1$, we have that $\mathrm{Nm}_{L_{n+1}/L_n} : L_{n+1}^\times/(L_{n+1}^\times)^t \longrightarrow L_n^\times/(L_n^\times)^t$ is in fact an isomorphism. □

From this we get the following corollary.

Corollary 3.3.11. *We have an isomorphism* $X_L^\times/(X_L^\times)^t \cong \varprojlim_n (L_n^\times/(L_n^\times)^t)$. *Moreover the map* $\varprojlim_n (L_n^\times/(L_n^\times)^t) \longrightarrow L^\times/(L^\times)^t$ *given by the projection map on the first component is an isomorphism.*

Proof. Let us first consider the short exact sequence

$$1 \longrightarrow \mu_t \longrightarrow L_n^\times \longrightarrow (L_n^\times)^t \longrightarrow 1$$

for $n \geq 1$. Then consider the functor $\varprojlim_n$ with transition maps given by $\mathrm{Nm}_{L_{n+1}/L_n}$. Since μ_t is finite, the Mittag-Leffler condition implies that this functor is exact on this short exact sequence and hence we have that

$$1 \longrightarrow \varprojlim_n \mu_t \longrightarrow \varprojlim_n L_n^\times \longrightarrow \varprojlim_n (L_n^\times)^t \longrightarrow 1.$$

In particular, we have that $\varprojlim_n L_n^\times/\varprojlim_n \mu_t \cong \varprojlim_n (L_n^\times)^t$. On the other hand we have that $\varprojlim_n L_n^\times/\varprojlim_n \mu_t \cong (\varprojlim_n L_n^\times)^t$, where the isomorphism is given by raising an element to the t-th power. Hence $(X_L^\times)^t \cong \varprojlim_n (L_n^\times)^t$.

Now notice that the natural map $X_L^\times/(X_L^\times)^t \cong \varprojlim_n L_n^\times/\varprojlim_n (L_n^\times)^t \longrightarrow \varprojlim_n (L_n^\times/(L_n^\times)^t)$ is injective. Herbrand's quotient gives us that $|X_L^\times/(X_L^\times)^t| = t^2 = |L_n^\times/(L_n^\times)^t|$ and by lemma 3.3.10 we have that $|\varprojlim_n (L_n^\times/(L_n^\times)^t)| = t^2$. Thus the natural map is in fact an isomorphism, $X_L^\times/(X_L^\times)^t \cong \varprojlim_n (L_n^\times/(L_n^\times)^t)$. The projection map on the first component of $\varprojlim_n (L_n^\times/(L_n^\times)^t)$, is an isomorphism by lemma 3.3.10. □

In particular, we have that the following diagram commutes:

$$\begin{tikzcd} X_L^\times \arrow[r] \arrow[d] & L^\times \arrow[d] \\ X_L^\times/(X_L^\times)^t \arrow[r, "\sim"] & L^\times/(L^\times)^t \end{tikzcd}$$

where the first horizontal map is given by the projection map on the first component and the second horizontal map is given by the isomorphism of corollary 3.3.11 followed by the projection map on the first component.

Definition 3.3.12. We define π_t to be a t-th root of π_1 in $X_L^\times$, which is in fact a uniformizer of X_L. Such an element exists by corollary 3.3.11 and the previous commutative diagram.

Lemma 3.3.13.

$$\frac{\pi^{1/t}}{\pi_t} \in \mathcal{O}_{\mathbb{E}_K}^\times.$$

Proof. Recall that $\pi_1 = \frac{1}{p-1}\sum_{\gamma\in\Delta}\chi(\gamma)^{-1}\gamma(\pi)$ and $\frac{\pi_1}{\pi} \equiv 1 \bmod \pi$. Hence the polynomial $X^t - \frac{\pi}{\pi_1}$ defined over $\mathcal{O}_{\mathbb{E}_K}$ is congruent to $X^t - 1 \bmod \pi$, which has a root $X = 1$ over $\mathbb{F}_q$. Moreover its derivative evaluated at $X = 1$ is non-zero $\bmod \pi$ and so by Hensel's lemma the polynomial has a root in $\mathcal{O}_{\mathbb{E}_K}^\times$. $\square$

Corollary 3.3.14. $\pi^{1/t}$ *is a uniformizer of* X_L.

Corollary 3.3.15.

$$\xi = \omega_{\tau_0,f}^{p^f-1-\sum_{i=0}^{f-1} c_{i-1}p^i}.$$

Proof. Recall from lemma 3.0.20, we have that $\xi|_{I_K} = \omega_{\tau_0,f}^{p^f-1-\sum_{i=0}^{f-1} c_{i-1}p^i}$. We also have from lemma 3.1.2 that the splitting field of ξ is given by $\mathbb{E}_K(\pi^{1/t})$ and we have from corollary 3.3.14 that $\mathbb{E}_K(\pi^{1/t}) \subset X_L$. Moreover the theory of field of norms gives an isomorphism $G_{X_L} \cong G_{L_\infty}$ and $G_{L_\infty} \subset \ker \xi$. Since $\mathrm{Gal}(L_\infty/K)$ is totally ramified, ξ has no unramified part. This shows that characters ξ and ψ have the same totally ramified splitting field and agree on inertia. Hence $\xi = \psi$ (as opposed to an unramified twist). $\square$

To summarize, we have the following:

$$
\begin{tikzcd}[arrows=-]
& M_\infty \arrow[d] & & X_M = X_L(z_i) \arrow[d] \\
M = L(\sqrt[p]{a_1}, ..., \sqrt[p]{a_f}) \arrow[ur] \arrow[d, "\text{splitting field of } c_\rho"'] & L_\infty \arrow[d] & & X_L = \mathbb{F}_{p^f}((\pi_t)) \arrow[d] \\
L = K(\sqrt[e]{-p}) \arrow[ur] \arrow[d, "\text{splitting field of } \psi"'] & K_\infty & & X_K \\
K = \mathbb{Q}_{p^f} \arrow[ur] & & &
\end{tikzcd}
$$

3.4 The wildly ramified splitting field as a composite of Artin-Schreier extensions

X_M is defined as the splitting field of the homomorphism $c'_\rho : G_{X_L} \longrightarrow \mathbb{F}_q$ and has degree $[X_M : X_L] = q$. As we saw in the previous section, it is the splitting field of the polynomial $X^q - X - \frac{H_i(\pi)}{\alpha_i}$. Moreover, $\mathrm{Gal}(X_M/X_L) \cong \mathbb{F}_q$ and therefore X_M is the composite of f Artin-Schreier subextensions. Write $\delta_i := \frac{H_i(\pi)}{\alpha_i}$ and recall that z_i is a root of the polynomial $X^q - X - \delta_i$. Let also ζ to be a primitive $p^f - 1$ root of unity and for some fixed $0 \leq j \leq f-1$ and $0 \leq d_j \leq p^f - 1$ let us write

$$\gamma_j := \sum_{k=0}^{f-1} (\zeta^{d_j} z_i)^{p^k}.$$

Then we have that $\gamma_j^p - \gamma_j = \zeta^{d_j}\delta_i$ and γ_j defines an Artin-Schreier subextension. In particular we have the following theorem;

Theorem 3.4.1. *Let* $\{\zeta^{d_0}, ..., \zeta^{d_{f-1}}\}$ *be a* $\mathbb{F}_p$*-basis of* $\mathbb{F}_q$*. Then* $X_M = X_L(\gamma_0, ..., \gamma_{f-1})$.

Proof. Recall from corollary 1.3.10, we have an inclusion preserving bijection

$$\{\text{subgroups of } X_L/(\mathrm{Frob}_p - 1)X_L\} \leftrightarrow \{\text{Artin-Schreier extensions of } X_L\},$$

where the bijection is given by $\Delta \mapsto X_L(\Delta')$. Here Δ' is the set of roots of the polynomials $X^p - X - a$, for $a \in \Delta$. Hence to find elements $\gamma_0, ..., \gamma_{f-1}$ such that $X_M = X_L(\gamma_0, ..., \gamma_{f-1})$, it suffices to find a basis for the subgroup A of $X_L/(\mathrm{Frob}_p - 1)X_L$ that corresponds to X_M by the above bijection.

Given $0 \le d < p^f - 1$, let

$$A_d := < \zeta^d \delta_i >_{\mathbb{F}_p} + (\mathrm{Frob}_p - 1)X_L$$

and consider

$$A := < \zeta^{d_j}\delta_i : 0 \le j \le f-1 >_{\mathbb{F}_p} + (\mathrm{Frob}_p - 1)X_L$$

as subgroups of $X_L/(\mathrm{Frob}_p - 1)X_L$. Then if the elements $\zeta^{d_j}\delta_i$ for $0 \le j \le f-1$ are linearly dependent over $\mathbb{F}_p$ in $A \subset X_L/(\mathrm{Frob}_p - 1)X_L$ then it would imply that there exist elements $a_{d_j} \in \mathbb{F}_p$ such that $\sum_{j=0}^{f-1} a_{d_j}\zeta^{d_j}\delta_i + x^p - x = 0$, for some $x \in X_L$. But notice that $v_{X_L}(\sum_{j=0}^{f-1} a_{d_j}\zeta^{d_j}\delta_i) = v_{X_L}(\delta_i)$. As we saw in proof of lemma 3.3.4, $v_{X_L}(\delta_i) = t(1-p) + s_i \not\equiv 0 \bmod p$ and by corollary 1.5.3 the polynomial $X^p - X + \sum_{j=0}^{f-1} a_{d_j}\zeta^{d_j}\delta_i$ is irreducible over X_L. Hence the elements are linearly independent. On the other hand, since $\{\zeta^{d_0}, ..., \zeta^{d_{f-1}}\}$ is an $\mathbb{F}_p$-basis of $\mathbb{F}_q$, any $\zeta^d\delta_i$ is a linear combination of $\{\zeta^{d_0}, ..., \zeta^{d_{f-1}}\}$. Thus $A_d \subseteq A$, for any $0 \le d < p^f - 1$.

Also for $0 \leq d, d' < p^f - 1$, we have that if $d \not\equiv d' \bmod \frac{p^f-1}{p-1}$ then A_d and $A_{d'}$ are different subgroups. Otherwise there would exist $a, b \in \mathbb{F}_p$ such that $a\zeta^d\delta_i + x^p - x = b\zeta^{d'}\delta_i$, for some $x \in X_L$. By the same reasoning as before, the polynomial $X^p - X + \delta_i(a\zeta^d - b\zeta^{d'})$ is irreducible over X_L since $v_{X_L}(\delta_i(a\zeta^d - b\zeta^{d'})) = v_{X_L}(\delta_i)$. Hence $a\zeta^d - b\zeta^{d'} = 0$. We can view $a = \zeta_{p-1}^{\alpha} = \zeta^{\alpha\frac{p^f-1}{p-1}}$ and $b = \zeta_{p-1}^{\beta} = \zeta^{\beta\frac{p^f-1}{p-1}}$. So $0 = a\zeta^d - b\zeta^{d'} = \zeta^{\alpha\frac{p^f-1}{p-1}+d} - \zeta^{\beta\frac{p^f-1}{p-1}+d'}$. But this is true if and only if $\alpha(p^f-1)+d(p-1) = \beta(p^f-1)+d'(p-1)$, if and only if $d \equiv d' \bmod \frac{p^f-1}{p-1}$. Thus given corollary 1.3.10, we have that A_d corresponds to an Artin-Schreier subextension of X_M. Moreover, we have constructed $\frac{p^f-1}{p-1}$ of them. On the other hand $\mathbb{F}_q$ has exactly $\frac{p^f-1}{p-1}$ $\mathbb{F}_p$ subgroups. As a result, we have found all the Artin-Schreier subextensions of X_M and we have shown that $A_d \subseteq A$. Hence $X_M = X_L(\gamma_0, ..., \gamma_{f-1})$. $\square$

Corollary 3.4.2. *Writing $X_{M_i} := X_L(\gamma_i)$, we have that X_M is the composite of X_{M_i} for $0 \leq i \leq f-1$ and $Gal(X_M/X_L) \cong \prod_{i=0}^{f-1} Gal(X_{M_i}/X_L) \cong (\mathbb{Z}/p\mathbb{Z})^f$, the isomorphism given by $g \mapsto (g|_{X_{M_i}})_{i=0}^{f-1}$. Notice that this isomorphism depends on the choice of basis $\{\zeta^{d_0}, ..., \zeta^{d_{f-1}}\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$.*

Let us now consider the following diagram:

$$\begin{tikzcd}
& \mathrm{Gal}(X_M/X_L) \cong \prod_{i=0}^{f-1} \mathrm{Gal}(X_{M_i}/X_L) \arrow[dl, "\sim"', "c'_{\rho,i}"] \arrow[dr, "\sim", "\theta"'] & \\
\mathbb{F}_q \cong (\mathbb{Z}/p\mathbb{Z})^f \arrow[rr, "\sim", "\iota"'] & & (\mathbb{Z}/p\mathbb{Z})^f
\end{tikzcd}$$

where the maps θ and ι are given by

$$\theta : g \longmapsto (g \cdot \gamma_j - \gamma_j)_{j=0}^{f-1}$$

$$\iota : x \longmapsto (-\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\zeta^{d_j} x))_{j=0}^{f-1}$$

Notice that for $g \in \mathrm{Gal}(X_M/X_L)$ we have that

$$g \cdot \gamma_j = \sum_{k=0}^{f-1} (\zeta^{d_j} g \cdot z_i)^{p^k} = \sum_{k=0}^{f-1} (\zeta^{d_j}(z_i - c'_{\rho,i}(g)))^{p^k}.$$

Thus

$$g \cdot \gamma_j - \gamma_j = -\sum_{k=0}^{f-1} (\zeta^{d_j} c'_{\rho,i}(g))^{p^k}$$

and the diagram commutes. As a result, we also have that the outer triangle of the following diagram also commutes:

$$\begin{tikzcd}
& G_{X_L} \arrow[d] \arrow[ddl, bend right] \arrow[ddr, bend left] & \\
& \mathrm{Gal}(X_M/X_L) \cong \prod_{i=0}^{f-1} \mathrm{Gal}(X_{M_i}/X_L) \arrow[dl, "\sim", "c'_{\rho,i}"'] \arrow[dr, "\sim", "\theta"'] & \\
k \arrow[rr, "\sim", "\iota"'] & & (\mathbb{Z}/p\mathbb{Z})^f
\end{tikzcd}$$

Hence we have the following lemma.

Lemma 3.4.3. *ker* $c'_{\rho,i} =$ *ker* θ, *as subgroups of* G_{X_L}.

Precomposing $c'_{\rho,i}$ with Art_{X_M/X_L} gives a map $c'_{\rho,i} \circ \mathrm{Art}_{X_M/X_L} : X_L^\times / \mathrm{Nm}_{X_M/X_L}(X_M^\times) \longrightarrow k$ and inflating to $X_L^\times$ we get $c'_{\rho,i} \circ \mathrm{Art}_{X_M/X_L} : X_L^\times \longrightarrow k$. We can do the same for the map θ and get $\theta \circ \mathrm{Art}_{X_M/X_L} : X_L^\times / \mathrm{Nm}_{X_M/X_L}(X_M^\times) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^f$. Therefore, we have the following corollary.

Corollary 3.4.4. *For* $\alpha \in X_L^\times$, *we have that* $c'_{\rho,i} \circ Art_{X_M/X_L}(\alpha) = 0$ *if and only if* $(\alpha, \zeta^{d_j}\delta_i] = 0$, *for all* $0 \leq j \leq f-1$.

Proof. From lemma 3.4.3 we have that $c'_{\rho,i} \circ \mathrm{Art}_{X_M/X_L}(\alpha) = 0$ if and only if $\theta \circ \mathrm{Art}_{X_M/X_L}(\alpha) = (\mathrm{Art}_{X_M/X_L}(\alpha) \cdot \gamma_j - \gamma_j)_{j=0}^{f-1} = 0$. That is if and only if $\mathrm{Art}_{X_M/X_L}(\alpha) \cdot$

$\gamma_j - \gamma_j = 0$, for $0 \leq j \leq f-1$. Since $\gamma_j^p - \gamma_j - \zeta^{d_j}\delta_i = 0$ defines an Artin-Schreier extension, we have that $\mathrm{Art}_{X_M/X_L}(\alpha) \cdot \gamma_j - \gamma_j = (\alpha, \zeta^{d_j}\delta_i]$. $\square$

3.5 Proof of duality in the equicharacteristic case

In this section we prove that $c'_{\rho,i} \circ \mathrm{Art}_{X_M/X_L}$ is dual to the set of elements $\{\overline{E}_p(a\pi_t^{m_j}) : 0 \leq j \leq f-1\}$, for $a \in \mathbb{F}_q^\times$. In section 3.1 of [7], the authors define $\lambda_\gamma \in \mathbb{F}_p[[\pi]]$ to be the unique t-th root of $\frac{\gamma(\pi)}{\chi(\gamma)\pi}$, which is congruent to 1 mod π, if $\gamma \in \Gamma_K$. Moreover, we have that the Laurent polynomial $H_i(\pi)$ satisfies $\lambda_\gamma^{s_{i-1}}\gamma(H_i(\pi)) \equiv H_i(\pi) \bmod \mathbb{F}_q[[\pi]]$ (section 4.1 of [7]). We first need the following intermediate results.

Lemma 3.5.1. *For $\gamma \in \Gamma$, the following congruences hold in $\mathbb{F}_q[[\pi]]$:*

- $\gamma(\pi_1) \equiv \chi(\gamma)\pi_1$ *mod* π_1^p
- $\gamma(\pi_1^{p-1}) \equiv \pi_1^{p-1}$ *mod* $\pi_1^{2(p-1)}$

Proof. Suppose $\chi(\gamma) \equiv 1 \bmod p$, that is $\gamma \in \Gamma_1$ and $\chi(\gamma) = 1 + \sum_{i=1}^{\infty} x_i p^i$. First notice that

$$\gamma(\pi) = (1+\pi)^{\chi(\gamma)} - 1 = (1+\pi)\prod_{i=1}^{\infty}(1+\pi^{p^i})^{x_i} - 1 \equiv 1 + \pi - 1 = \pi \bmod \pi_1^p.$$

Moreover for any $\gamma \in \Gamma$, $\gamma(\pi^p) = (1+\pi^p)^{\chi(\gamma)} - 1$ and we have that Γ acts on $\mathcal{O}_{\mathbb{E}_K}/\pi^p$. In particular, Γ_1 acts trivially. Thus the action of Γ on $\mathcal{O}_{\mathbb{E}_K}/\pi^p$ factors through $\Gamma/\Gamma_1 \cong (\mathbb{Z}/p\mathbb{Z})^\times$ and the action of Δ on $\mathcal{O}_{\mathbb{E}_K}/\pi^p$ is the same as its action via the isomorphism $\Delta \cong \Gamma/\Gamma_1$. On the other hand, $\mathcal{O}_{\mathbb{E}_K}/\pi^p$ is a vector space over $\mathbb{F}_p$ and is isomorphic to $\bigoplus_{i=0}^{p-1} \mathcal{O}_{\mathbb{E}_K}\pi_1^i \bmod \pi^p$. We also have from proposition 3.3.7 that for $\delta \in \Delta$, $\delta(\pi_1) = \chi(\delta)\pi_1$ and thus for any $\gamma \in \Gamma$, $\gamma(\pi_1) = \chi(\gamma)\pi_1 \bmod \pi_1^p$. In particular, for any integer i we have that $\gamma(\pi_1^i) = \chi(\gamma)^i\pi_1^i \bmod \pi_1^p$.

For the second congruence, we can use the first part to write $\gamma(\pi_1) = \chi(\gamma)\pi_1 + a\pi_1^p$, for some $a \in \mathcal{O}_{\mathbb{E}_K}$. Taking $p-1$ powers we get

$$\begin{aligned}
\gamma(\pi_1)^{p-1} &= (\chi(\gamma)\pi_1 + a\pi_1^p)^{p-1} \\
&= \pi_1^{p-1}(\chi(\gamma) + a\pi_1^{p-1})^{p-1} \\
&= \pi_1^{p-1}\sum_{k=0}^{p-1}\binom{p-1}{k}\chi(\gamma)^{p-1-k}(a\pi_1^{p-1})^k \\
&= \pi_1^{p-1} + a\pi_1^{2(p-1)}\sum_{k=1}^{p-1}\chi(\gamma)^{p-1-k}(a\pi_1^{p-1})^{k-1},
\end{aligned}$$

which gives the result. $\square$

Using this, we can prove the following.

Proposition 3.5.2. $\frac{\pi^{\frac{s_{i-1}}{t}} H_i(\pi)}{\pi_t^{-p^f+1+s_{i-1}}}$ *mod* $\pi^{p-1}\mathbb{F}_q[[\pi_t]]$ *is fixed under the action of* Γ_K.

Proof. From lemma 3.5.1, we have that $\gamma(\pi_1) \equiv \chi(\gamma)\pi_1 \bmod \pi_1^{p-1}$, for $\gamma \in \Gamma$. Then we have that

$$\gamma(\frac{\pi}{\pi_1}) \equiv \frac{\gamma(\pi)\pi}{\chi(\gamma)\pi_1\pi} \bmod \pi_1^{p-1}.$$

Using 3.3.13 and the fact that the terms in the congruence are units, this is true if and only if $\gamma(\frac{\pi^{1/t}}{\pi_t}) \equiv \frac{\pi^{1/t}}{\pi_t}\lambda_\gamma \bmod \pi_1^{p-1}\mathbb{F}_q[[\pi_t]]$ or $\gamma(\frac{\pi^{s_{i-1}/t}}{\pi_t^{s_{i-1}}}) \equiv \frac{\pi^{s_{i-1}/t}}{\pi_t^{s_{i-1}}}\lambda_\gamma^{s_{i-1}} \bmod \pi_1^{p-1}\mathbb{F}_q[[\pi_t]]$. Multiplying with $H_i(\pi)$ we get that

$$\gamma(\frac{\pi^{s_{i-1}/t}}{\pi_t^{s_{i-1}}})\frac{H_i(\pi)}{\lambda_\gamma^{s_{i-1}}} \equiv \frac{\pi^{s_{i-1}/t}}{\pi_t^{s_{i-1}}}H_i(\pi) \bmod \mathbb{F}_q[[\pi_t]].$$

Using the congruence $\gamma(H_i(\pi)) \equiv \frac{H_i(\pi)}{\lambda_\gamma^{s_{i-1}}} \bmod \mathbb{F}_q[[\pi]]$,

$$\gamma(\frac{\pi^{s_{i-1}/t}H_i(\pi)}{\pi_t^{s_{i-1}}}) \equiv \frac{\pi^{s_{i-1}/t}}{\pi_t^{s_{i-1}}}H_i(\pi) \bmod \mathbb{F}_q[[\pi_t]].$$

Multiplying with π_1^{p-1}, we have

$$\gamma(\frac{\pi^{s_{i-1}/t}H_i(\pi)}{\pi_t^{s_{i-1}}})\pi_1^{p-1} \equiv \frac{\pi^{s_{i-1}/t}}{\pi_t^{s_{i-1}}}H_i(\pi)\pi_1^{p-1} \bmod \pi^{p-1}\mathbb{F}_q[[\pi_t]].$$

From lemma 3.5.1, we have that $\gamma(\pi_1^{p-1}) \equiv \pi_1^{p-1} \bmod \pi^{2(p-1)}$ and so

$$\gamma(\frac{\pi^{s_{i-1}/t}H_i(\pi)}{\pi_t^{s_{i-1}}})\gamma(\pi_1^{p-1}) \equiv \gamma(\frac{\pi^{s_{i-1}/t}H_i(\pi)}{\pi_t^{s_{i-1}}})\pi_1^{p-1} \bmod \pi^{p-1}\mathbb{F}_q[[\pi_t]].$$

Hence we get that

$$\gamma(\frac{\pi^{s_{i-1}/t}H_i(\pi)}{\pi_t^{-p^f+1+s_{i-1}}}) \equiv \frac{\pi^{s_{i-1}/t}H_i(\pi)}{\pi_t^{-p^f+1+s_{i-1}}} \bmod \pi^{p-1}\mathbb{F}_q[[\pi_t]].$$

□

We also need the following result.

Lemma 3.5.3. *Suppose $a \in \mathbb{F}_q[[\pi]]$ is fixed under the action of Γ_K. Then we have that $a \in \mathbb{F}_q$.*

Proof. Consider the isomorphism $\mathbb{F}_q((\pi)) \cong X_{\mathbb{Q}_q}$ and interpret the element $a = (a_n)_{n\in\mathbb{N}}$ as a norm compatible sequence of $\varprojlim_n \mathbb{Q}_q(\zeta_{p^n})$. Since a is fixed under the action of Γ_K, we have that $a_n \in \mathbb{Q}_q$ for all n. Hence we have that $a_n = \mathrm{Nm}_{\mathbb{Q}_q(\zeta_{p^{n+1}})/\mathbb{Q}_q(\zeta_{p^n})}(a_{n+1}) = a_{n+1}^p$. This implies that for any integer m, we have that $a_{n+m}^{p^m} = a_n$ and hence $a_n^{1/p^m} = a_{n+m} \in \mathbb{Q}_q$. But then this implies that a_n is either equal to 0 or a $(q-1)$-st root of unity and so is a. □

From the previous results we can deduce the following.

Corollary 3.5.4.

$$\pi^{s_{i-1}/t}H_i(\pi) \equiv \pi_t^{-p^f+1+s_{i-1}} \ \mathit{mod}\ \mathcal{O}_{X_L}.$$

Proof. From lemma 3.5.2 we have that $\frac{\pi^{s_{i-1}/t}H_i(\pi)}{\pi_t^{-p^f+1+s_{i-1}}} \bmod \pi^{p-1}\mathbb{F}_q[[\pi_t]]$ is fixed under the action of Γ_K. Hence from lemma 3.5.3 we have that $\frac{\pi^{s_{i-1}/t}H_i(\pi)}{\pi_t^{-p^f+1+s_{i-1}}} \equiv 1 \bmod \pi^{p-1}\mathbb{F}_q[[\pi_t]]$. Thus $\pi^{s_{i-1}/t}H_i(\pi) \equiv \pi_t^{-p^f+1+s_{i-1}} \bmod \pi_t^{s_{i-1}}\mathbb{F}_q[[\pi_t]]$. □

As a result, we can prove the main result of this section.

Theorem 3.5.5. *For any basis $B := \{\zeta^{d_0}, ..., \zeta^{d_{f-1}}\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, $a \in \mathbb{F}_q$ and $0 \le k \le f-1$, we have that*

$$(\overline{E}_p(a\pi_t^{p^f-1-s_j}), \zeta^{d_k}\delta_i] = \begin{cases} 0, & \text{if } j \neq i-1 \\ \\ Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(p^f-1-s_{i-1})\zeta^{d_k}), & \text{if } j = i-1. \end{cases}$$

Moreover, we can choose our basis B so that

$$(\overline{E}_p(a\pi_t^{p^f-1-s_{i-1}}), \zeta^{d_0}\delta_i] = Tr_{\mathbb{F}_q/\mathbb{F}_p}(a(p^f-1-s_{i-1})\zeta^{d_0}) \neq 0.$$

Proof. By the previous corollary we have that $\zeta^{d_k}\delta_i = \zeta^{d_k}\pi^{s_{i-1}/t}H_i(\pi) \equiv \zeta^{d_k}\pi_t^{-p^f+1+s_{i-1}} \mod \mathcal{O}_{X_L}$. Since the symbol $(\cdot,\cdot]$ is additive in its second argument and $\overline{E}_p(a\pi_t^{p^f-1-s_j})$ is a unit in X_L, we have that

$$(\overline{E}_p(a\pi_t^{p^f-1-s_j}), \zeta^{d_k}\delta_i] = (\overline{E}_p(a\pi_t^{p^f-1-s_j}), \zeta^{d_k}\pi_t^{-p^f+1+s_{i-1}}].$$

Recall that we have from theorem 1.3.14 that $(a,b] = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{res}_{\pi_t}(\frac{b}{a}\frac{da}{d\pi_t}))$. In particular,

$$\frac{1}{\overline{E}_p(a\pi_t^{p^f-1-s_j})}\frac{d(\overline{E}_p(a\pi_t^{p^f-1-s_j}))}{d\pi_t} = \sum_{n=0}^{\infty}(p^f-1-s_j)a^{p^n}\pi_t^{(p^f-1-s_j)p^n-1}.$$

Hence

$$\frac{\zeta^{d_k}\pi_t^{-p^f+1+s_{i-1}}}{\overline{E}_p(a\pi_t^{p^f-1-s_j})}\frac{d(\overline{E}_p(a\pi_t^{p^f-1-s_j}))}{d\pi_t} = \zeta^{d_k}\pi_t^{-p^f+1+s_{i-1}}\sum_{n=0}^{\infty}(p^f-1-s_j)a^{p^n}\pi_t^{(p^f-1-s_j)p^n-1}.$$

As a result possibly non-zero residues of the above expression are given when the exponent satisfies $(p^f-1-s_j)p^n-1-p^f+1+s_{i-1} = -1$. That is we are looking for solutions to the equation $(p^f-1-s_j)p^n-(p^f-1)+s_{i-1} = 0$.

First suppose $j \neq i-1$. If $n > 0$ and the equation has a solution then $s_{i-1} \equiv p-1 \mod p$. But $s_{i-1} \equiv c_i \mod p$ and by strong genericity, $c_i < p-1$. Thus we have a contradiction. If $n = 0$, then by the primitiveness assumption the equation does not have a solution. In the case where $j = i-1$, then we have that the equation reduces to $(p^n - 1)(p^f - 1 - s_{i-1}) = 0$. It is clear that if $n > 0$, the equation has no solution since $s_{i-1} < p^f - 1$. Thus the last case remaining is when $j = i-1$ and $n = 0$, in which case we get $(\overline{E}_p(a\pi_t^{p^f-1-s_{i-1}}), \zeta^{d_k}\delta_i] = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a(p^f - 1 - s_{i-1})\zeta^{d_k}) = (p^f - 1 - s_{i-1})\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\zeta^{d_k} a)$.

For the moreover part, recall that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \twoheadrightarrow \mathbb{F}_p$ and the kernel has dimension p^{f-1}. Notice that the map given by $x \mapsto ax$ for $x \in \mathbb{F}_q$ is an automorphism and so there exists $\tilde{x} \in \mathbb{F}_q$ such that $a\tilde{x}$ is not in the kernel of the trace map. Thus taking $\zeta^{d_0} = \tilde{x}$, we get the result. $\square$

Theorem 3.5.6. *Given $a \in \mathbb{F}_q^{\times}$, we have that for $j \in S$*

$$c'_{\rho,i} \circ Art_{X_M/X_L}(\overline{E}_p(a\pi_t^{m_j})) = \begin{cases} 0, & \text{if } j \neq i \\ \\ \neq 0, & \text{if } j = i. \end{cases}$$

Moreover, we have that $\{\overline{E}_p(a\pi_t^{m_j}) : 0 \leq j \leq f-1, j \neq i\}$ lies in the image of Nm_{X_M/X_L}, whereas the element $\overline{E}_p(a\pi_t^{m_i})$ does not.

Proof. By corollary 3.4.4 we have that $c'_{\rho,i} \circ \mathrm{Art}_{X_M/X_L}(\overline{E}_p(a\pi_t^{p^f-1-s_j})) = 0$ if and only if $(\overline{E}_p(a\pi_t^{p^f-1-s_j}), \zeta^{d_k}\delta_i] = 0$ for all $0 \leq k \leq f-1$. Hence the result follows from theorem 3.5.5 and the fact that $m_j = p^f - 1 - s_{j-1}$. Since Art_{X_M/X_L} gives an isomorphism $X_M^{\times}/\mathrm{Nm}_{X_M/X_L}(X_M^{\times}) \cong \mathrm{Gal}(X_M/X_L)$, we have that $\{\overline{E}_p(a\pi_t^{m_j}) : 0 \leq j \leq f-1, j \neq i\}$ is a subset of $\mathrm{Nm}_{X_M/X_L}(X_M^{\times})$, whereas the element $\overline{E}_p(a\pi_t^{m_i})$ is not. $\square$

3.6 Proof of duality in the mixed characteristic case

Let us write $[\cdot] : \mathbb{F}_q^\times \longrightarrow L^\times$ for the Teichmüller map. In this section we show that given $a \in \mathbb{F}_q^\times$, $\{E_p([a]\pi_L^{m_j}) \bmod U_L^{p^f-1-t}(L^\times)^p \cap U_L^t : 0 \leq j \leq f-1, j \neq i\}$ is a subset of $\mathrm{Nm}_{M/L}(\mathcal{O}_M^\times) \bmod U_L^{p^f-1-t}(L^\times)^p \cap U_L^t$. Recall that our assumptions imply that L contains ζ_p and by lemma 3.3.1 we have that $M \cap (\mathbb{Q}_p)_\infty = \mathbb{Q}_p(\zeta_p)$ and $M_n \cap L_\infty = L_n$. Hence for an element $(x_n)_{n\in\mathbb{N}} \in X_M = \varprojlim_n M_n$ (with transition maps given by norms) we have that its norm is given by

$$\mathrm{Nm}_{X_M/X_L}((x_n)_{n\in\mathbb{N}}) = (\mathrm{Nm}_{M_n/M_n\cap L_\infty}(x_n))_{n\in\mathbb{N}} = (\mathrm{Nm}_{M_n/L_n}(x_n))_{n\in\mathbb{N}}.$$

We then have the following result.

Proposition 3.6.1.

$$Nm_{X_M/X_L}(X_M^\times) \subset \varprojlim_n Nm_{M_n/L_n}(M_n^\times),$$

where transition maps are given by norms.

Proof. Notice that for $n' \leq n$ we have by the definition of X_M that $x_{n'} = \mathrm{Nm}_{M_n/M_{n'}}(x_n)$ and so we have the relation

$$\begin{aligned}
\mathrm{Nm}_{M_{n'}/L_{n'}}(x_{n'}) &= \mathrm{Nm}_{M_{n'}/M_{n'}\cap L_\infty}(\mathrm{Nm}_{M_n/M_{n'}}(x_n)) \\
&= \mathrm{Nm}_{M_n/M_{n'}\cap L_\infty}(x_n) \\
&= \mathrm{Nm}_{M_n\cap L_\infty/M_{n'}\cap L_\infty}(\mathrm{Nm}_{M_n/M_n\cap L_\infty}(x_n)) \\
&= \mathrm{Nm}_{L_n/L_{n'}}(\mathrm{Nm}_{M_n/L_n}(x_n)).
\end{aligned}$$

That is, the following diagram commutes:

$$\begin{array}{ccc} M_n & \xrightarrow{\mathrm{Nm}_{M_n/M_{n'}}} & M_{n'} \\ {\scriptstyle \mathrm{Nm}_{M_n/L_n}}\downarrow & & \downarrow{\scriptstyle \mathrm{Nm}_{M_{n'}/L_{n'}}} \\ L_n & \xrightarrow{\mathrm{Nm}_{L_n/L_{n'}}} & L_{n'} \end{array}$$

We have that

$$\varprojlim_n \mathrm{Nm}_{M_n/L_n}(M_n^\times) = \left\{ (\mathrm{Nm}_{M_n/L_n}(x_n))_n \in \prod_n (L_n)^\times \middle| \substack{\mathrm{Nm}_{L_{n+1}/L_n}(\mathrm{Nm}_{M_{n+1}/L_{n+1}}(x_{n+1}))= \\ \mathrm{Nm}_{M_n/L_n}(x_n)} \right\}$$

On the other hand we have

$$\mathrm{Nm}_{X_M/X_L}(X_M^\times) = \left\{ (\mathrm{Nm}_{M_n/L_n}(x_n))_n \in \prod_n (L_n)^\times \middle| \mathrm{Nm}_{M_{n+1}/M_n}(x_{n+1}) = x_n \right\}$$

and if $\mathrm{Nm}_{M_{n+1}/M_n}(x_{n+1}) = x_n$ then

$$\mathrm{Nm}_{M_n/L_n}(x_n) = \mathrm{Nm}_{M_n/L_n}(\mathrm{Nm}_{M_{n+1}/M_n}(x_{n+1})) = \mathrm{Nm}_{L_{n+1}/L_n}(\mathrm{Nm}_{M_{n+1}/L_{n+1}}(x_{n+1}))$$

$\square$

As a result we have the following result.

Lemma 3.6.2. *Let* $(\cdot)_1 : X_L = \varprojlim_n L_n \longrightarrow L$ *denote the projection map on first component. Then we have that for* $a \in \mathbb{F}_q$, $\{(\overline{E}_p(a\pi_t^{m_j}))_1 : 0 \leq j \leq f-1, j \neq i\}$ *is a subset of* $Nm_{M/L}(\mathcal{O}_M^\times)$.

Proof. In corollary 3.5.6 we have shown that $\{\overline{E}_p(a\pi_t^{m_j}) : 0 \leq j \leq f-1, j \neq i\}$ lies in the image of Nm_{X_M/X_L}. By proposition 3.6.1, we have the result. $\square$

Winterberger in his paper [28] defines the following. Given an APF extension N'/N, let

$$i(N'/N) := \sup \{i \geq -1 : G_N^i G_{N'} = G_N\}.$$

Let us write $Q_n := \mathbb{Q}_p(\zeta_{p^n})$. Recall also that the cyclotomic tower $Q_\infty := \underset{n\geq 0}{\cup} Q_n$ is an APF extension by a result of Sen [23]. We would like to calculate $i(Q_{n+1}/Q_n)$. Consider a character $\epsilon : Q_n^\times \longrightarrow \mathbb{C}^\times$. Then by continuity, it has an open kernel and so there is a least integer $f(\epsilon) \geq 0$ such that ϵ is trivial on the unit group $U_{Q_n}^{f(\epsilon)}$. This integer $f(\epsilon)$ is called the ***conductor exponent*** of ϵ and if ϖ_n is a uniformizer for Q_n then $\varpi_n^{f(\epsilon)}$ is called the ***conductor*** of ϵ. Then we have the following lemma.

Lemma 3.6.3. *Consider a character $\epsilon : Q_n^\times \longrightarrow \mathbb{C}^\times$ and its pull back to $W_{Q_n}^{ab}$ under the Artin map. Then $f(\epsilon)$ is the least integer $m \geq 0$ such that ϵ is trivial on $G_{Q_n}^m$.*

Proof. Using the Artin map one has an isomorphism $Q_n^\times \cong W_{Q_n}^{\mathrm{ab}}$. Moreover, for $i \geq 0$ we have that $G_{Q_n}^i \subset I_{Q_n} \subset W_{Q_n} \longrightarrow W_{Q_n}^{\mathrm{ab}}$. Hence we can consider the character ϵ as a character of $G_{Q_n}^i$. On the other hand since the Artin map transforms the filtration by the $U_{Q_n}^i$ into the filtration by the $G_{Q_n}^i$, we have that ϵ as a character of $G_{Q_n}^i$ factors through $U_{Q_n}^i$. $\square$

Let us now consider a character $\epsilon_{n+1} : \mathbb{Q}_p^\times \longrightarrow \mathbb{C}^\times$ of conductor p^{n+1}. That is ϵ_{n+1} factors through $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$. Writing $\epsilon_{n+1}|_{G_{Q_n}}$ for the restriction of ϵ_{n+1} to the subgroup $\mathrm{Gal}(Q_{n+1}/Q_n)$ of $\mathrm{Gal}(Q_{n+1}/Q_0) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$, by the previous lemma we have that $f(\epsilon_{n+1}|_{G_{Q_n}})$ is the least positive integer such that $G_{Q_n}^{f(\epsilon_{n+1}|_{G_{Q_n}})} \subset G_{Q_{n+1}}$. We then have the following.

Lemma 3.6.4.

$$i(Q_{n+1}/Q_n) = f(\epsilon_{n+1}|_{G_{Q_n}}) - 1.$$

Proof. We have that $i(Q_{n+1}/Q_n) = \sup\{i \geq -1 : G_{Q_n}^i G_{Q_{n+1}} = G_{Q_n}\}$ and using the fact that upper numbering respects quotients the condition $G_{Q_n}^i G_{Q_{n+1}} = G_{Q_n}$ translates to $\mathrm{Gal}(Q_{n+1}/Q_n)^i = \mathrm{Gal}(Q_{n+1}/Q_n)$. On the other hand $f(\epsilon_{n+1}|_{G_{Q_n}})$ is the least positive integer such that $\mathrm{Gal}(Q_{n+1}/Q_n)^{f(\epsilon_{n+1}|_{G_{Q_n}})}$ is trivial. Since $\mathrm{Gal}(Q_{n+1}/Q_n)$ is cyclic of order p, $\mathrm{Gal}(Q_{n+1}/Q_n)^i$ is either the whole group or trivial. Hence $f(\epsilon_{n+1}|_{G_{Q_n}}) - 1 \leq i(Q_{n+1}/Q_n) < f(\epsilon_{n+1}|_{G_{Q_n}})$. By the theorem of Hasse-Arf we have that the image of $G_{Q_n}^{i(Q_{n+1}/Q_n)}$ in the quotient $\mathrm{Gal}(Q_{n+1}/Q_n)$ is the same as the image of $G_{Q_n}^{f(\epsilon_{n+1}|_{G_{Q_n}})-1}$ and so we get the result. □

We can extend the notion of conductor exponent to a character of a representation of a Galois group G over $\mathbb{C}$. Given such a character ϵ we set

$$f(\epsilon) = \sum_{i=0}^{\infty} \frac{\text{codim } V^{G_i}}{[G_0 : G_i]}$$

(see [24] chapter VI §2 for more information).

Lemma 3.6.5. *Let ϵ be a character of a representation V over $\mathbb{C}$ of a Galois group G. Then one has that*

$$f(\epsilon) = \int_{-1}^{\infty} \textit{codim } V^{G^s} ds.$$

Proof. The sum $f(\epsilon) = \sum_{i=0}^{\infty} \frac{\text{codim } V^{G_i}}{[G_0:G_i]}$ is in fact equal to $\int_{-1}^{\infty} \frac{\text{codim } V^{G_u}}{[G_0:G_u]} du = \int_{-1}^{\infty} \frac{\text{codim } V^{G^{\Phi(u)}}}{[G_0:G_u]} du$ because the integrand is constant on intervals $(i-1, i]$. But then notice that letting $s := \Phi(u)$ we have that $ds = \frac{1}{[G_0:G_u]} du$, which gives the result. □

As a result we have reduced the problem to calculating $f(\epsilon_{n+1}|_{G_{Q_n}})$. To calculate this we will make use of the following result.

Proposition 3.6.6. *Let F/E be a finite Galois extension with Galois group G and H a subgroup of G corresponding to the subextension E'/E with corresponding residue field subextension $k_{E'}/k_E$. Let also $\delta_{E'/E}$ be the discriminant of E'/E. If ψ is a character of H and ψ^* the character induced on G, then*

$$f(\psi^*) = v_E(\delta_{E'/E})\psi(1) + [k_{E'} : k_E] f(\psi).$$

Proof. This is the corollary of proposition 4 from chapter VI, §2 of [24]. □

Proposition 3.6.7.

$$i(Q_{n+1}/Q_n) = p^n - 1.$$

Proof. From proposition 3.6.6 we have that $f((\epsilon_{n+1}|_{G_{Q_n}})^*) = v_{Q_0}(\delta_{Q_n/Q_0}) + f(\epsilon_{n+1}|_{G_{Q_n}})$. Moreover we have that $(\epsilon_{n+1}|_{G_{Q_n}})^* = \mathrm{Ind}_{G_{Q_n}}^{G_{Q_0}}(\epsilon_{n+1}|_{G_{Q_n}}) = (\mathrm{Ind}_{G_{Q_n}}^{G_{Q_0}} 1)\epsilon_{n+1} = \bigoplus_{1\leq i\leq \phi(p^n)} \eta_i\epsilon_{n+1}$, where $\{\eta_1, ..., \eta_{\phi(p^n)}\}$ are the characters of $\mathrm{Gal}(Q_n/Q_0)$. Recall that $f(\epsilon_{n+1}) = n+1$ and by lemma 3.6.3 this is the least integer $m \geq 0$ such that ϵ_{n+1} is trivial on $G_{Q_0}^m$. Similarly n is the least integer $m \geq 0$ such that η_i is trivial on $G_{Q_0}^m$ for all i. Using also the fact that Q_m/Q_0 are totally ramified for all m we have that $((\epsilon_{n+1}|_{G_{Q_n}})^*)^{G_{Q_0}^s}$ is trivial for $-1 \leq s \leq n$ and equal to $(\epsilon_{n+1}|_{G_{Q_n}})^*$ otherwise. So using lemma 3.6.5 we have that $f((\epsilon_{n+1}|_{G_{Q_n}})^*) = \int_{-1}^{\infty} \mathrm{codim}\ ((\epsilon_{n+1}|_{G_{Q_n}})^*)^{G_{Q_0}^s} ds = \phi(p^n)(n+1)$.

Let $h(X) := \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$ which is the minimal polynomial of ζ_{p^n} over Q_0. Then we have that $\delta_{Q_n/Q_0} = (\mathrm{Nm}_{Q_n/Q_0}(h'(\zeta_{p^n})))$. In particular, $h'(\zeta_{p^n}) = \frac{p^n\zeta_{p^n}^{p^n-1}}{\zeta_{p^n}^{p^{n-1}}-1}$ and so $\mathrm{Nm}_{Q_n/Q_0}(h'(\zeta_{p^n})) = \mathrm{Nm}_{Q_n/Q_0}(\frac{p^n\zeta_{p^n}^{p^n-1}}{\zeta_{p^n}^{p^{n-1}}-1}) = \frac{p^{n\phi(p^n)}\mathrm{Nm}_{Q_n/Q_0}(\zeta_{p^n})^{p^n-1}}{\mathrm{Nm}_{Q_n/Q_0}(\zeta_p-1)}$. But $\mathrm{Nm}_{Q_n/Q_0}(\zeta_{p^n}) = 1$ since h has constant coefficient equal to 1. Also $\mathrm{Nm}_{Q_n/Q_0}(\zeta_p-1) = \mathrm{Nm}_{Q_1/Q_0}(\mathrm{Nm}_{Q_n/Q_1}(\zeta_p-1)) = \mathrm{Nm}_{Q_1/Q_0}(\zeta_p-1)^{p^{n-1}} = p^{p^{n-1}}$, since the minimal polynomial of $\zeta_p - 1$ over Q_0 has constant coefficient equal to p. Hence $v_{Q_0}(\delta_{Q_n/Q_0}) = v_{Q_0}(p^{n\phi(p^n)-p^{n-1}}) = n\phi(p^n) - p^{n-1}$.

As a result we have that $f(\epsilon_{n+1}|_{G_{Q_n}}) = f((\epsilon_{n+1}|_{G_{Q_n}})^*) - v_{Q_0}(\delta_{Q_n/Q_0}) = \phi(p^n)(n+1) - (n\phi(p^n) - p^{n-1}) = p^n$. Hence using lemma 3.6.4 we get the result. □

From this result we can deduce the following.

Corollary 3.6.8.

$$i(L_{n+1}/L_n) \geq (p^n - 1)t.$$

Proof. The extension L_n/Q_n has no wild ramification. Hence $P_{L_n} = P_{Q_n}$ and $G^u_{Q_n} \subset G_{L_n}$, for all $u > 0$. So we can write $G^u_{Q_n} = \varprojlim_{E/Q_n} \mathrm{Gal}(E/Q_n)_{\Psi_{E/Q_n}(u)} = \varprojlim_{E/L_n} \mathrm{Gal}(E/L_n)_{\Psi_{E/Q_n}(u)}$. We also have that $\mathrm{Gal}(L_n/Q_n)_u = 0$ for all $u \geq 1$ and $[\mathrm{Gal}(L_n/Q_n)_0 : \mathrm{Gal}(L_n/Q_n)_u] = \#I(L_n/Q_n) = t$ for all $u > 0$. Thus $\Phi_{L_n/Q_n}(ut) = \int_0^{ut}[\mathrm{Gal}(L_n/Q_n)_0 : \mathrm{Gal}(L_n/Q_n)_s]^{-1}ds = \int_0^{ut}(\#I(L_n/Q_n))^{-1}ds = u$. Hence $\Psi_{L_n/Q_n}(u) = ut$ and using proposition 1.1.3, $\Psi_{E/Q_n}(u) = \Psi_{E/L_n} \circ \Psi_{L_n/Q_n}(u) = \Psi_{E/L_n}(ut)$. As a result we have that $G^u_{Q_n} = \varprojlim_{E/L_n} \mathrm{Gal}(E/L_n)_{\Psi_{E/L_n}(ut)} = G^{ut}_{L_n}$.

From proposition 3.6.7 we have that $i(Q_{n+1}/Q_n) = \sup\{i \geq -1 : G^i_{Q_n} G_{Q_{n+1}} = G_{Q_n}\} = p^n - 1$. Moreover we have that $G_{L_i} = G_{Q_i} \cap G_L$ for $i = n, n+1$ and $G^t_{Q_n} = G^{it}_{L_n} \subset G_L$, which implies $G^{it}_{L_n} G_{L_{n+1}} = G^i_{Q_n}(G_{Q_{n+1}} \cap G_L) = (G^i_{Q_n} G_{Q_{n+1}}) \cap G_L = G_{Q_n} \cap G_L = G_{L_n}$. Hence $i(L_{n+1}/L_n) \geq i(Q_{n+1}/Q_n)t = (p^n - 1)t$. $\square$

Recall that in lemma 3.6.2 we have shown that $\{(\overline{E}_p(a\pi_t^{m_j}))_1 : 0 \leq j \leq f-1, j \neq i\}$ is a subset of $\mathrm{Nm}_{M/L}(\mathcal{O}_M^\times)$. Recall also that the componentwise addition in the field of norms X_L is defined by $(x+y)_m = \lim_{n \longrightarrow \infty} \mathrm{Nm}_{L_n/L_m}(x_n + y_n)$. We can now give a lower bound on the valuation of the error term for which the norm map $\mathrm{Nm}_{L_{n+1}/L_n}$ fails to be a homomorphism.

Proposition 3.6.9. *Let $n \geq 0$ and $\alpha, \beta \in \mathcal{O}_{L_{n+1}}$. Then we have that*

$$v_{L_n}(Nm_{L_{n+1}/L_n}(\alpha+\beta) - Nm_{L_{n+1}/L_n}(\alpha) - Nm_{L_{n+1}/L_n}(\beta)) \geq \frac{(p^n-1)(p^f-1)}{p}.$$

Proof. From [28] proposition 2.2.1, we have that $v_{L_n}(\mathrm{Nm}_{L_{n+1}/L_n}(\alpha+\beta) - \mathrm{Nm}_{L_{n+1}/L_n}(\alpha) - \mathrm{Nm}_{L_{n+1}/L_n}(\beta)) \geq \frac{i(L_{n+1}/L_n)(p-1)}{p}$. Hence from corollary 3.6.8 we get the result. $\square$

Corollary 3.6.10. *Let $m, k \geq 0$ and $\alpha, \beta \in \mathcal{O}_{L_{m+k}}$. Then we have that*

$$Nm_{L_{m+k}/L_m}(\alpha+\beta) \equiv Nm_{L_{m+k}/L_m}(\alpha) + Nm_{L_{m+k}/L_m}(\beta) \ mod\ \pi_L^{p^f-1-t}.$$

Proof. In proposition 3.6.9 we have shown that $v_{L_n}(\mathrm{Nm}_{L_{n+1}/L_n}(\alpha+\beta)-\mathrm{Nm}_{L_{n+1}/L_n}(\alpha)-\mathrm{Nm}_{L_{n+1}/L_n}(\beta)) \geq \frac{(p^n-1)(p^f-1)}{p}$. Moreover notice that $\frac{(p^n-1)(p^f-1)}{p} = p^{n-1}(p^f-1-\frac{p^f-1}{p^n}) \geq p^{n-1}(p^f-1-\frac{p^f-1}{p-1}) = p^{n-1}(p^f-1-t) = v_{L_n}(\pi_L^{p^f-1-t})$, which is true for all $n \geq 1$. As a result we have that for all $n \geq 1$, $\mathrm{Nm}_{L_{n+1}/L_n}(\alpha+\beta) \equiv \mathrm{Nm}_{L_{n+1}/L_n}(\alpha) + \mathrm{Nm}_{L_{n+1}/L_n}(\beta) \bmod \pi_L^{p^f-1-t}$ and by successive applications of $\mathrm{Nm}_{L_{n+1}/L_n}$ for $m \leq n \leq m+k-1$ we get the result. $\square$

We are now in a position to prove the main result of this section.

Theorem 3.6.11. *Given $a \in \mathbb{F}_q^\times$, $\{E_p([a]\pi_L^{m_j}) \bmod U_L^{p^f-1-t}(L^\times)^p \cap U_L^t : 0 \leq j \leq f-1, j \neq i\}$ is a subset of $Nm_{M/L}(\mathcal{O}_M^\times) \bmod U_L^{p^f-1-t}(L^\times)^p \cap U_L^t$.*

Proof. We have that E_p is given on the quotient $\pi_L^t\mathcal{O}_L/\pi_L^{p^f-1-t}\mathcal{O}_L$ by $E_p(x) \equiv \sum_{n=0}^{p-1}\frac{x^n}{n!}$. Notice that if $\alpha, \beta \in \mathcal{O}_{X_L}$ then from corollary 3.6.10 we have that for $m \geq 0$,

$$\begin{aligned}(\alpha+\beta)_m &= \lim_{k\longrightarrow\infty}\mathrm{Nm}_{L_{m+k}/L_m}(\alpha_{m+k}+\beta_{m+k})\\ &\equiv \lim_{k\longrightarrow\infty}(\mathrm{Nm}_{L_{m+k}/L_m}(\alpha_{m+k})+\mathrm{Nm}_{L_{m+k}/L_m}(\beta_{m+k})) \bmod \pi_L^{p^f-1-t}\\ &= \alpha_m+\beta_m.\end{aligned}$$

Suppose $\{\alpha^{(n)} : 1 \leq n \leq r\} \subset \mathcal{O}_{X_L}$. Then we have that

$$\begin{aligned}(\sum_{1\leq n\leq r}\alpha^{(n)})_m &= \lim_{k\longrightarrow\infty}\mathrm{Nm}_{L_{m+k}/L_m}((\sum_{1\leq n\leq r-1}\alpha^{(n)})_{m+k}+(\alpha^{(r)})_{m+k})\\ &\equiv \lim_{k\longrightarrow\infty}(\mathrm{Nm}_{L_{m+k}/L_m}((\sum_{1\leq n\leq r-1}\alpha^{(n)})_{m+k})+\alpha_m^{(r)} \bmod \pi_L^{p^f-1-t}.\end{aligned}$$

By induction we have that this is congruent to

$$\begin{aligned}\lim_{k\longrightarrow\infty}(\mathrm{Nm}_{L_{m+k}/L_m}((\sum_{1\leq n\leq r-1}\alpha_{m+k}^{(n)}))+\alpha_m^{(r)} &\equiv \sum_{1\leq n\leq r-1}\lim_{k\longrightarrow\infty}(\mathrm{Nm}_{L_{m+k}/L_m}(\alpha_{m+k}^{(n)}))+\alpha_m^{(r)}\\ &= \sum_{1\leq n\leq r}\alpha_m^{(n)} \bmod \pi_L^{p^f-1-t}.\end{aligned}$$

Hence

$$
\begin{aligned}
(\overline{E}_p(a\pi_t^{m_j}))_1 &\equiv (\sum_{n=0}^{p-1} \frac{(a\pi_t^{m_j})^n}{n!})_1 \\
&\equiv \sum_{n=0}^{p-1} \frac{[a]^n(\pi_t)_1^{(m_j)n}}{n!} \bmod \pi_L^{p^f-1-t}.
\end{aligned}
$$

By definition and lemma 3.3.9, $(\pi_t)_1 = (\pi_1)_1^{1/t} \equiv \pi_L \bmod \pi_L^{p^f}$. As a result we have that

$$
\begin{aligned}
(\overline{E}_p(a\pi_t^{m_j}))_1 &\equiv \sum_{n=0}^{p-1} \frac{[a]^n\pi_L^{(m_j)n}}{n!} \\
&\equiv E_p([a]\pi_L^{m_j}) \bmod \pi_L^{p^f-1-t}.
\end{aligned}
$$

But then by lemma 3.6.2 we get the result. □

From this we can deduce the following duality result.

Theorem 3.6.12. *Given $a \in \mathbb{F}_q^\times$, we have that for $j \in S$*

$$
c_{\rho,i} \circ Art_{M/L}(E_p([a]\pi_L^{m_j})) = \begin{cases} 0, & \textit{if } j \neq i \\ \\ \neq 0, & \textit{if } j = i. \end{cases}
$$

In particular we have that $c_{\rho,i} \in L_{\{i-2\}} \cong \mathbb{F}_q B_i$ is in ker ν_{j-1} for all $j \in S \setminus \{i\}$. This proves conjecture 2.2.19 in the strongly generic case.

Proof. From proposition 3.0.21 and theorem 3.0.22 we get that $L_{\{i-2\}} \cong \mathbb{F}_q B_i$. From theorem 3.6.11 and the fact that $m_j = p^f - 1 - s_{j-1}$, we get the result. □

Bibliography

[1] L. Barthel and R. Livné, *Irreducible modular representations of GL_2 of a local field*, Duke Math. J., vol. 75(1994), 261-292.

[2] L. Berger, *An introduction to the theory of p-adic representations, 2004.*

[3] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol.I, Progr. Math. 86, 333-400, Birkhäuser, Boston, 1990.

[4] C. Breuil, *Representations of Galois and of GL_2 in characteristic p*, Cours à l'université de Columbia, automne 2007.

[5] O. Brinon and B. Conrad, *CMI summer school notes on p-adic Hodge theory (preliminary version), 2009.*

[6] K. Buzzard, F. Diamond, and F. Jarvis, *On Serre's conjecture for mod l Galois representations over totally real fields*, Duke Math. J., vol. 155, Number 1 (2010), 105-161.

[7] S. Chang and F. Diamond, *Extensions of rank one (ϕ, Γ)-modules and crystalline representations*, Compositio Math. 147 (2011), 375-427.

[8] L. Dembélé, F. Diamond, and D. Roberts, *Serre weights and wild ramification in two-dimensional Galois representations*, Preprint.

[9] I.B. Fesenko and S.V. Vostokov, *Local fields and their extensions*, Second Edition 2001.

[10] J.-M. Fontaine, *Exposé III*, Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque 223 (1994), 321-347.

[11] ———, *Le corps des périodes p-adiques*, Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque 223 (1994), 59-111.

[12] ———, *Représentations ℓ-adiques potentiellement semi-stables*, Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque 223 (1994), 321-347.

[13] ———, *Représentations p-adiques des corps locaux I*, The Grothendieck Festschrift, Vol. II, 249-309, Birkhäuser, Boston, 1990.

[14] ———, *Représentations p-adiques semi-stables*, Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque 223 (1994), 113-184.

[15] T. Gee, T. Liu, and D. Savitt, *The Buzzard-Diamond-Jarvis conjecture for unitary groups*, J. Amer. Math. Soc. 27 (2014), no. 2, 389435.

[16] P. Gille and T. Szamuely, *Central simple algebras and galois cohomology*, Cambridge University Press, 2006.

[17] F. Gouvêa, *p-adic numbers: An introduction*, Springer Verlag 1993.

[18] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. 178 (2009), 485-504.

[19] ———, *Serre's modularity conjecture (II)*, Invent. Math. 178 (2009), 505-586.

[20] D. Kracht, *Applications of the artin-hasse exponential series and its generalizations to finite algebra groups*, PHD thesis, Kent State University, 2011.

[21] S. Mattarei, *Exponential functions in prime characteristic*, Aequationes Math. 71 (2006), no. 3, 311-317.

[22] S. Sen, *Continuous cohomology and p-adic Galois representations*, Invent. Math., vol. 62, 1980-81, p. 89-116.

[23] ———, *Ramification in p-adic Lie extensions*, Invent. Math., vol. 17, 1972, p. 44-50.

[24] J.-P. Serre, *Local fields*, Springer, 1980, vol.67, Graduate Texts in Mathematics.

[25] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., vol. 15, 1972, no. 4, p. 259-331.

[26] ———, *Sur les représentations modulaires de degré 2 de Gal*($\overline{\mathbb{F}}_p/\mathbb{Q}_p$), Duke Math. J., vol. 54 (1987), 179-230.

[27] J. Tate, *p-divisible groups*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, p. 158-183.

[28] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux; applications*, Ann. scient., Éc. Norm. Sup. (4) 16 (1983), 59-89.